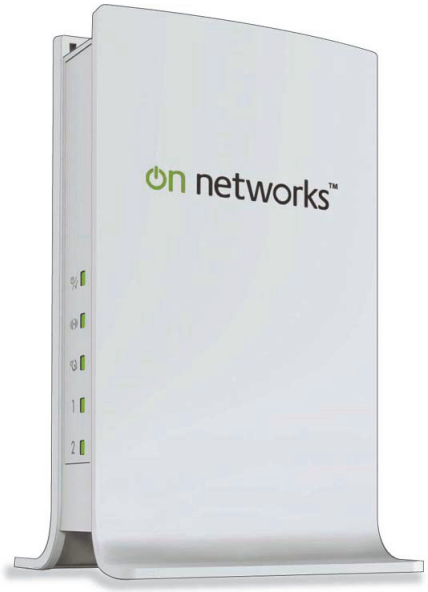
on networks™
Easy, Reliable & Secure

N150 WLAN-Router (N150R)

Benutzerhandbuch



August 2012
202-11156-01
v1.0

Marken

Marken- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber. Informationen können ohne vorherige Ankündigung geändert werden.

Zur Verbesserung des internen Designs, des Betriebs und/oder der Zuverlässigkeit behält On Networks sich das Recht vor, die in diesem Dokument beschriebenen Produkte ohne vorherige Ankündigung zu ändern. On Networks lehnt im Zusammenhang mit dem Einsatz oder der Anwendung der hier beschriebenen Produkte oder Schaltpläne jegliche Haftung ab.

Dieses Symbol wurde in Übereinstimmung mit der EU-Richtlinie 2002/96/EG über Elektro- und Elektronik-Altgeräte (WEEE-Richtlinie) hier angebracht. Die Entsorgung dieses Produkts innerhalb der Europäischen Union sollte in Übereinstimmung mit den in Ihrem Land zur Implementierung der WEEE-Richtlinie geltenden Gesetzen gehandhabt werden.

Inhalt

Kapitel 1 Hardware-Konfiguration

Lieferumfang Ihres Routers 7
Positionieren des Routers 7
Hardware-Funktionen 8
Vorderseite 8
Rückseite 9
Typenschild 10

Kapitel 2 Erste Schritte

Vorbereitung der Router-Konfiguration 12
Verwenden der Standard-TCP/IP-Eigenschaften für DHCP 12
Austausch der vorhandenen Modem- und Routerhardware 12
Sammeln von ISP-Informationen 12
Anmelden am Router 13
Anmeldung nicht erfolgreich 14
Manuelle Abmeldung 14
Anmeldearten 14
Startbildschirm (Dashboard) 15
EZ Setup-Assistent 16
Herstellen einer Verbindung mit einem WLAN-Netzwerk 17
WPS-Methode 17
Manuelle Methode 18

Kapitel 3 Router-Konfiguration

Internetkonfiguration (Grundeinstellungen) 20
Voreingestellte Sicherheit 22
Grundlagen der WLAN-Sicherheit 23
Deaktivieren des SSID-Broadcast 23
Einschränkung des Zugriffs über MAC-Adressen 23
WLAN-Sicherheitsoptionen 24
WiFi-Setup 24
Überprüfen jedes Geräts in Ihrem Netzwerk 24
Anzeigen oder Ändern der WLAN-Konfiguration 25
Felder auf dem Bildschirm Wireless Settings (WLAN-Konfiguration) . . . 25
Ändern der WPA-Sicherheitsoption und Passphrase 26
Internet-Port 27
DMZ-Standardserver 28
Ändern der MTU-Größe 28

LAN-Ports 30
Verwenden des Routers als DHCP-Server 32
Adressreservierung 33
QoS (Quality of Service)-Konfiguration 34

Kapitel 4 Sicherheitseinstellungen

Firewall-Regeln zur Steuerung des Netzwerkzugangs 40
Eingangsregeln (Portweiterleitung) 40
Ausgangsregeln (Dienstsperren) 40
Konfigurieren der Seitensperrung 41
Löschen eines Stichworts oder einer Domain 41
Angeben eines vertrauenswürdigen Computers 42
Konfigurieren der Dienstsperre 42
Einstellen der Zeitzone 43
Zeitliches Planen von Diensten 44
Konfigurieren von E-Mail-Warnmeldungen 45
Portweiterleitung und Port-Triggering 46
Grundlegende Informationen zum Remote-Computerzugriff 46
Port-Triggering zum Öffnen eingehender Ports 48
Portweiterleitung zur Zulassung externer Hostkommunikation 49
Unterschiede zwischen Portweiterleitung und Port-Triggering 50
Konfigurieren der Portweiterleitung an lokale Server 51
Hinzufügen eines benutzerdefinierten Diensts 52
Bearbeiten oder Löschen eines Portweiterleitungseintrags 53
Konfigurieren des Port-Triggering 53

Kapitel 5 Netzwerkverwaltung

Aktualisieren der Router-Firmware 57
Automatische Firmwareprüfung 57
Beenden der automatischen Firmwareprüfung 58
Manuelle Suche nach Firmware-Aktualisierungen 58
Sichern der Einstellungen 59
Sichern 60
Wiederherstellen 60
Löschen 60
Ändern des Passworts 60
Passwortwiederherstellung 61
Anzeigen des Routerstatus 62
Internet-Porteinstellungen 62
LAN-Port (Lokale Ports) 63
Modem 63
Access Point 63
Anzeigen der Statistik 64
Verbindungsstatus 65
Anzeigen von angeschlossenen Geräten 65
Protokolle 66

Kapitel 6 Erweiterte Einstellungen

Erweiterte WLAN-Konfiguration 68
Einschränkung des WLAN-Zugriffs über MAC-Adressen 69
WLAN-Repeating (WDS) 71
WLAN-Repeating 72
Konfigurieren der Basisstation 73
Konfigurieren eines Repeaters 74
Dynamisches DNS 75
Statische Routen 76
Fernsteuerung 78
Universal Plug and Play 79

Kapitel 7 Fehlerbehebung

Tipps 82
Sequenz zum Neustart des Netzwerks 82
Überprüfen der Netzwerkkabel 82
WLAN-Einstellungen 82
Netzwerkeinstellungen 82
Behebung von Fehlern im Zusammenhang mit LEDs 83
Die Power-/Test-LED ist aus 83
Power-/Test-LED bleibt gelb 83
Die LEDs erlöschen nicht 84
Die Internet- oder Netzwerkanschluss-LEDs leuchten nicht 84
Anmeldung am Router nicht möglich 84
Es kann keine Internetverbindung hergestellt werden 85
Fehlerbehebung bei PPPoE 87
Fehlerbehebung im Zusammenhang mit dem Internetzugriff 87
Änderungen werden nicht gespeichert 88
Verbindung über WLAN 88
WLAN-Signalstärke 88
Wiederherstellen der Werkseinstellungen und des Passworts 89
Fehlerbehebung im Netzwerk mithilfe des Ping-Dienstprogramms 89
Testen des LAN-Pfads zum Router 89
Testen des Pfads vom Computer zu einem Remote-Gerät 90

Anhang A Zusatzinformationen

Werkseitige Voreinstellungen 93
Technische Daten 94

Anhang B Konformitätserklärung

Stichwortverzeichnis

Hardware-Konfiguration

1

Ihr Router

In diesem Kapitel wird die Konfiguration der Hardware erläutert. Wenn Sie den N150R-Router bereits konfiguriert haben, können Sie dieses Kapitel überspringen. In Kapitel 2 wird die Konfiguration der Internetverbindung erläutert.

Dieses Kapitel enthält die folgenden Abschnitte:

- *Lieferumfang Ihres Routers*
- *Positionieren des Routers*
- *Hardware-Funktionen*

Lieferumfang Ihres Routers

Öffnen Sie den Karton, und nehmen Sie den Router, die Kabel und die Installationsanleitung heraus.

N150 WLAN-Router | Netzwerkkabel | Netzteil

Abbildung 1. Überprüfen des Packungsinhalts

Ihre Lieferung umfasst die folgenden Artikel:

- N150 WLAN-Router (N150R)
- Netzteil und Netzkabel (Stecker je nach Region unterschiedlich)
- Netzwerkkabel (Kategorie 5)
- Installationsanleitung mit Anweisungen zu Kabeln und Routerkonfiguration

Falls einer dieser Teile fehlt, beschädigt ist oder zu einem anderen Modell gehört, wenden Sie sich bitte an Ihren On Networks-Fachhändler. Bewahren Sie den Karton sowie das Original-Verpackungsmaterial für den Fall auf, dass Sie das Produkt zu einem späteren Zeitpunkt zur Reparatur einsenden müssen.

Positionieren des Routers

Der Router ermöglicht Ihnen den Zugriff auf Ihr Netzwerk von praktisch jedem Standort innerhalb des WLAN-Radius. Durch die richtige Aufstellung des Routers können Sie jedoch dazu beitragen, den WLAN-Radius vergrößern. Zum Beispiel kann die Reichweite des Signals durch die Stärke und Anzahl der Wände, die das Signal durchdringt, eingeschränkt werden. Beste Ergebnisse erzielen Sie bei der Wahl folgender Standorte für Ihren Router:

- Möglichst nahe am Zentrum des Bereichs, in dem sich Ihre Computer und anderen Geräte befinden, und vorzugsweise in Sichtverbindung zu allen Wireless-Geräten
- In der Nähe einer Steckdose und in Reichweite der Netzwerkkabel Ihrer kabelgebundenen Computer
- In erhöhter Position wie beispielsweise auf einem Wandregal, wobei sich zwischen dem Router und den anderen Geräten möglichst wenige Wände und Decken befinden sollten

- Nicht in der Nähe von elektronischen Geräten, die Störungen verursachen können Zu Geräten, die Störungen verursachen können, zählen Deckenventilatoren, Alarmanlagen, Mikrowellengeräte, PCs, Basisstationen von schnurlosen Telefonen oder schnurlose 2,4-GHz-Telefone.
- Nicht in der Nähe größerer Metalloberflächen wie massiven Metalltüren oder Aluminiumteilen. Größere Flächen aus Materialien wie Glas, Ziegelstein oder Beton sowie Dämmplatten, Aquarien oder Spiegel können das Signal ebenfalls beeinträchtigen.

Bei Verwendung mehrerer Access Points empfiehlt es sich, nicht die Funkfrequenzkanäle zu wählen, die bereits von den benachbarten Access Points verwendet werden, um Störungen zu reduzieren. Der empfohlene Abstand der Kanäle benachbarter Access Points beträgt 5 Kanäle (verwenden Sie beispielsweise die Kanäle 1 und 6 oder 6 und 11).

Hardware-Funktionen

Nehmen Sie sich einen Moment Zeit, um sich mit dem Typenschild, der Vorder- und Rückseite und den Seiten vertraut zu machen, bevor Sie den Router anschließen. Achten Sie dabei besonders auf die LEDs auf der Vorderseite.

Vorderseite

An der Vorderseite des Routers befinden sich die in der folgenden Abbildung dargestellten LEDs und Symbole.

Abbildung 2. Vorderansicht des Routers

Tabelle 1. Beschreibung der LEDs auf der Vorderseite

LED	Beschreibung
Power/ Test	• **Leuchtet grün**. Der Router wird mit Strom versorgt. • **Blinkt grün**. Der Router startet. • **Aus**. Der Router wird nicht mit Strom versorgt.
WLAN	• **Blinkt grün**. Daten werden über die drahtlose Verbindung übertragen oder empfangen. • **Aus**. Die WLAN-Funktion ist deaktiviert.
Internet	• **Leuchtet grün**. Es besteht eine Internetverbindung. • **Blinkt grün**. Es werden Daten über den Internetanschluss übertragen. • **Aus**. Keine Internetverbindung.
Netzwerk (1-2)	• **Leuchtet grün**. Am LAN-Port wurde eine Netzwerkverbindung mit einem Gerät erkannt, z. B. einem Computer. • **Blinkt grün**. Daten werden übertragen oder empfangen. • **Aus**. An diesem Port wurde keine Verbindung erkannt.

Rückseite

An der Rückseite befinden sich die in der folgenden Abbildung dargestellten Verbindungen.

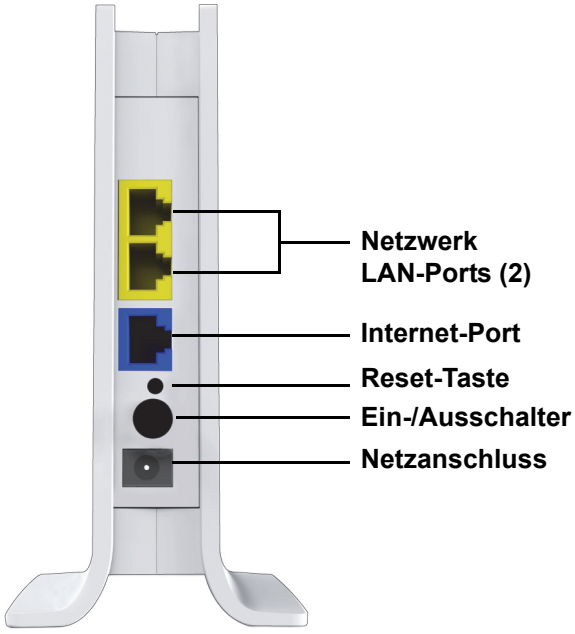


Abbildung 3. Router, Rückansicht

Weitere Informationen zum Zurücksetzen der Werkseinstellungen finden Sie unter *Werkseitige Voreinstellungen* auf Seite 93.

Typenschild

Auf dem Typenschild an der Unterseite des Routers werden Name und Passwort des voreingestellten WLAN-Netzwerks, Anmeldeinformationen, MAC-Adresse und Seriennummer angegeben.

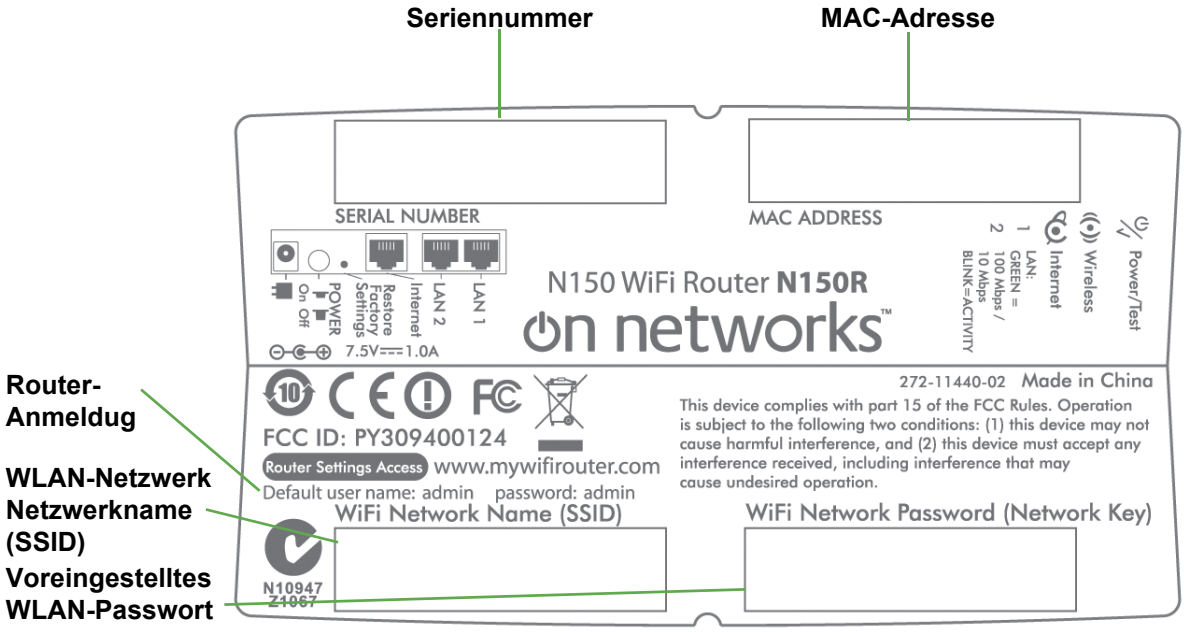

Seriennummer
MAC-Adresse
SERIAL NUMBER
MAC ADDRESS
N150 WiFi Router N150R
on networks
Router-Anmeldug
WLAN-Netzwerk Netzwerkname (SSID)
Voreingestelltes WLAN-Passwort
FCC ID: PY309400124
Router Settings Access www.mywifirouter.com
Default user name: admin password: admin
WiFi Network Name (SSID)
WiFi Network Password (Network Key)
272-11440-02 Made in China
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Abbildung 4. Auf dem Typenschild werden eindeutige Informationen zu Ihrem Gerät angegeben

2 Erste Schritte

Zugriff auf den Router

In diesem Kapitel wird erläutert, wie Sie sich beim Router anmelden und den Startbildschirm (Dashboard) aufrufen, um die Interneteinstellungen anzuzeigen oder zu ändern, und wie Sie eine Verbindung mit dem WLAN-Netzwerk herstellen. Dieses Kapitel enthält die folgenden Abschnitte:

- *Vorbereitung der Router-Konfiguration*
- *Anmelden am Router*
- *Startbildschirm (Dashboard)*
- *EZ Setup-Assistent*
- *Herstellen einer Verbindung mit einem WLAN-Netzwerk*

Vorbereitung der Router-Konfiguration

Sie können Ihren Router wie unter *EZ Setup-Assistent* auf Seite 16 beschrieben mit dem Setup-Assistenten oder manuell wie unter *Internetkonfiguration (Grundeinstellungen)* beschrieben konfigurieren. Bevor Sie mit der Konfiguration beginnen, müssen Sie jedoch Ihre ISP-Informationen zur Hand haben und sicherstellen, dass die Laptops, PCs und anderen Geräte im Netzwerk mit den hier beschriebenen Einstellungen eingerichtet sind.

Hinweis: Für Apple-Computer und Linux-PCs muss die Konfiguration manuell erfolgen.

Verwenden der Standard-TCP/IP-Eigenschaften für DHCP

Wenn Sie den Computer für die Verwendung einer statischen IP-Adresse konfiguriert haben, müssen Sie die Einstellungen zurücksetzen, sodass DHCP (Dynamic Host Configuration Protocol) verwendet wird.

Austausch der vorhandenen Modem- und Routerhardware

Um die vorhandene Modem- und Routerhardware auszutauschen, müssen Sie sie vom Anschluss trennen, bevor Sie mit der Konfiguration des Routers beginnen.

Sammeln von ISP-Informationen

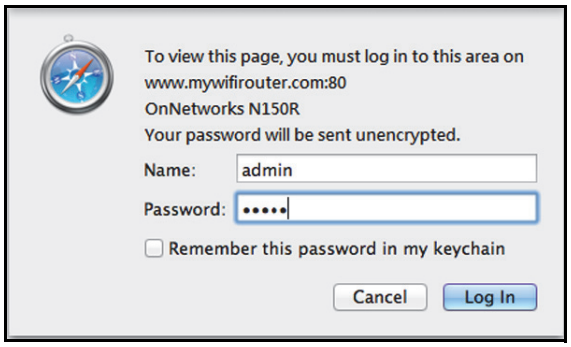
Sie benötigen die folgenden Informationen, um den Router einrichten und die Internetkonfiguration prüfen zu können. Normalerweise müssten Sie alle Informationen, die Sie zur Verbindung mit dem Internet benötigen, von Ihrem Internet-Provider (ISP) erhalten haben. Wenn Sie diese Informationen nicht finden können, bitten Sie Ihren ISP darum, diese bereitzustellen. Wenn die Internetverbindung Ihres Routers steht, benötigen Sie das Anmeldeprogramm des ISPs auf Ihrem Computer nicht mehr für den Internetzugriff. Beim Start einer Internetanwendung meldet der Router Sie automatisch an.

- Aktives Internetdienstkonto
- Die Konfigurationsdaten vom ISP für Ihr Konto
  - Benutzername und Passwort vom ISP zur Anmeldung
  - DNS-Serveradressen (Domain Name Server) des Internetdienstanbieters
  - feste oder statische IP-Adresse
  - Host- und Domainnamen
  - Je nach Einstellung Ihres Internetkontos durch den ISP benötigen Sie für eine manuelle Konfiguration eventuell Informationen zu einigen der folgenden Einstellungen:
    - Werte für VPI (Virtual Path Identifier) und VCI (Virtual Channel Identifier)
    - Multiplexverfahren
    - Host- und Domainnamen

Anmelden am Router

➢ **Sie können sich beim Router anmelden, um Einstellungen anzuzeigen oder zu ändern oder um den Router zu konfigurieren.**

1. Geben Sie **http://192.168.1.1** in die Adresszeile Ihres Browsers ein, und drücken Sie die **Enter-Taste**, um das Anmeldefenster aufzurufen. Sie können auch eine der beiden folgenden Adressen eingeben, um eine Verbindung zu Ihrem Router herzustellen: **http://www.mywifirouter.com**.

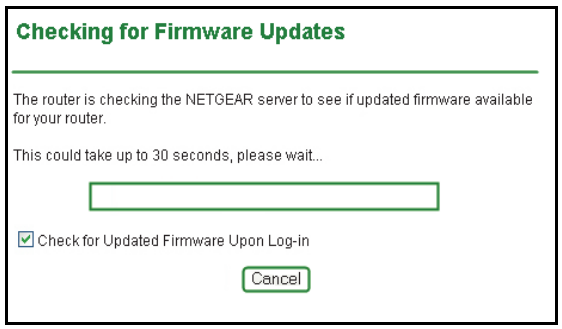


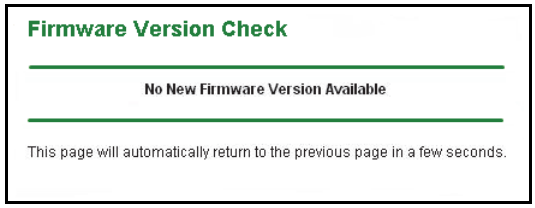
2. Geben Sie **admin** als Benutzernamen und **admin** als Passwort ein. Beide Wörter müssen kleingeschrieben werden.

Hinweis: Der Benutzername und das Passwort des Routers unterscheiden sich eventuell vom Benutzernamen und Passwort für die Anmeldung zum Herstellen einer Internetverbindung. Weitere Informationen finden Sie in *Anmeldearten* auf Seite 14.

Wenn Sie bei der Anmeldung mit dem Internet verbunden sind, wird der Bildschirm **Firmware Upgrade Assistant** (Assistent für die Aktualisierung der Firmware) angezeigt, sodass Sie eine Aktualisierung der Firmware durchführen können.

Bei der Anmeldung wird die links dargestellte Meldung angezeigt, wenn vom Router eine neuere Firmware-Version erkannt wird. Falls keine neue Firmware verfügbar ist, wird die rechts dargestellte Meldung angezeigt.


Checking for Firmware Updates
The router is checking the NETGEAR server to see if updated firmware available for your router.
This could take up to 30 seconds, please wait...
Check for Updated Firmware Upon Log-in
Cancel


Firmware Version Check
No New Firmware Version Available
This page will automatically return to the previous page in a few seconds.

3. Klicken Sie zur Aktualisierung auf die neue Firmware auf **Yes** (Ja), um zuzulassen, dass der Router die neue Firmware-Datei von On Networks herunterlädt und installiert.

WARNUNG:

Achten Sie beim Hochladen der Firmware auf den N150R-Router darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

Nach dem Hochladen der Firmware wird der Router neu gestartet. Der Aktualisierungsvorgang dauert in der Regel ungefähr eine Minute.

Anmeldung nicht erfolgreich

➢ **Gehen Sie folgendermaßen vor, wenn die Anmeldeaufforderung nicht angezeigt wird:**

1. Prüfen Sie die LEDs auf der Vorderseite des Routers, um sicherzustellen, dass der Router richtig angeschlossen wurde, eingeschaltet ist und das Netzwerkkabel zwischen dem Computer und dem Router an einen LAN-Port angeschlossen ist.
2. Wenn Sie das Netzwerkkabel angeschlossen und kurz darauf mit dem Browser die URL des Routers aufgerufen haben, benötigt Ihr Computer eventuell eine Weile zur Erkennung der LAN-Verbindung. Starten Sie Ihren Browser neu, und versuchen Sie es erneut.
3. Falls beim WLAN-Zugriff auf den Router Probleme auftreten, empfiehlt On Networks, während der Konfiguration ein Netzwerkkabel für die Verbindung mit dem Computer zu verwenden, damit Sie sich am Router anmelden können.
4. Falls Sie keine Verbindung zum Router herstellen können, überprüfen Sie die Eigenschaften des Internetprotokolls (TCP/IP) der Netzwerkverbindung in der Systemsteuerung Ihres Computers. Stellen Sie dort sicher, dass Ihr Computer IP-Adresse *und* DNS-Server-Adresse automatisch bezieht. Weitere Informationen finden Sie in der Dokumentation Ihres Computers.

Manuelle Abmeldung

Die Router-Benutzeroberfläche stellt einen Abmeldebefehl bereit. Dieser befindet sich im unteren Bereich des Router-Menüs. Melden Sie sich ab, wenn Sie den Computer voraussichtlich für längere Zeit verlassen.

Anmeldearten

Es gibt drei verschiedene Anmeldearten mit unterschiedlichem Zweck. Es ist wichtig, dass Sie den Unterschied verstehen, damit Sie wissen, wann Sie welche Anmeldung verwenden müssen.

- Bei der **Router-Anmeldung** erfolgt die Anmeldung über die Routerbenutzeroberfläche. Weitere Informationen zu dieser Anmeldung finden Sie unter *Anmelden am Router* auf Seite 13.
- Bei der **ISP-Anmeldung** werden Sie beim Internet-Provider angemeldet. Ihr Provider hat Ihnen diese Anmeldedaten in einem Brief oder auf andere Weise zukommen lassen. Wenn Ihnen diese Anmeldeinformationen nicht vorliegen, wenden Sie sich bitte an Ihren Provider.
- Mit **WLAN-Netzwerkname und Passphrase** melden Sie sich bei Ihrem WLAN-Netzwerk an. Diese Anmeldung ist vorkonfiguriert; die Daten befinden sich auf dem Typenschild an der Unterseite Ihres Geräts. Weitere Informationen finden Sie in *WiFi-Setup* auf Seite 24.

Startbildschirm (Dashboard)

Mithilfe der Router-Benutzeroberfläche können Sie die Einstellungen des Routers anzeigen und ändern. Die linke Spalte verfügt über Menüs, und die rechte bietet Online-Hilfe. Die mittlere Spalte ist der Bildschirm für die aktuelle Menüoption.

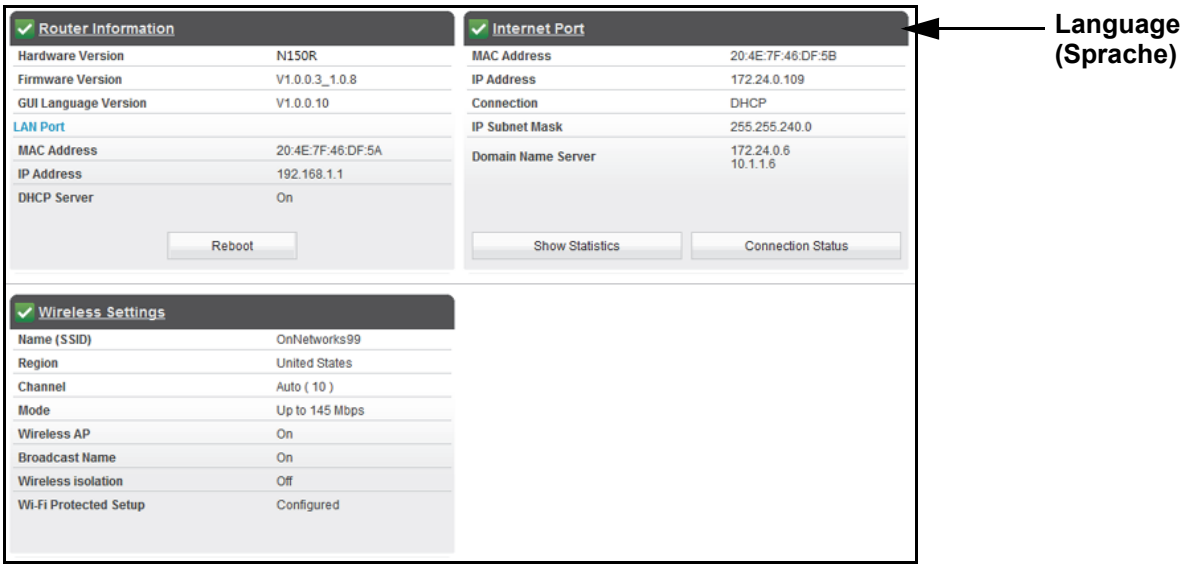


Abbildung 5. Dashboard (Startbildschirm)

- **EZ Setup-Assistent:** Geben Sie die Sprache und den Ort an; automatische Erkennung der Internetverbindung. Siehe *EZ Setup-Assistent* auf Seite 16.
- **WPS Setup (WPS-Konfiguration):** Herstellen einer Verbindung mit dem sicheren WLAN-Netzwerk ohne Eingabe des Passworts. Siehe *Herstellen einer Verbindung mit einem WLAN-Netzwerk*.
- Registerkarte **Setup** (Konfiguration): Konfiguration, Aktualisierung und Überprüfung des ISP sowie der WLAN-Einstellungen Ihres Routers. Siehe *Internetkonfiguration (Grundeinstellungen)*. Weitere Informationen zu voreingestellten und grundlegenden Sicherheitseinstellungen finden Sie unter *Kapitel 3, Router-Konfiguration*.

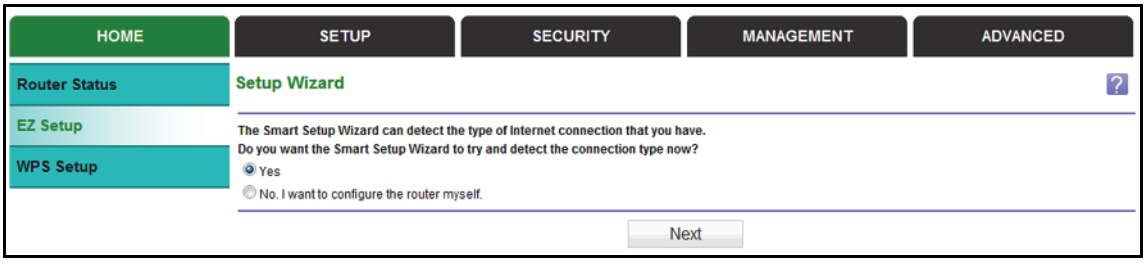
- Registerkarte **Security** (Sicherheit): Anzeige und Konfiguration der Firewall-Einstellungen Ihres Routers, damit keine fragwürdigen Inhalte auf Ihre Computer gelangen. Siehe *Kapitel 4, Sicherheitseinstellungen*.
- Registerkarte **Management** (Verwaltung): Administration des Routers und Netzwerks. Siehe *Kapitel 5, Netzwerkverwaltung*.
- Registerkarte **Advanced** (Erweitert): Konfigurieren des Routers für besondere Situationen, etwa wenn Remote-Zugriff über IP oder Domainname über das Internet benötigt wird. Siehe *Kapitel 6, Erweiterte Einstellungen*. Für die Verwendung dieses Menüs sind solide Netzwerkkenntnisse erforderlich.
- **Other Links** (Andere Links): Auf der Supportwebsite erhalten Sie Informationen, Hilfe und Produktdokumentationen. Sie können diese Links verwenden, wenn Sie eine Verbindung mit dem Internet hergestellt haben.

EZ Setup-Assistent

Sie können sich am Router anmelden und mit **EZ Setup** (Einfache Konfiguration) Ihre Internetverbindung konfigurieren.

➢ **So verwenden Sie den Setup-Assistenten:**

1. Wählen Sie oben im Menü des Routers die Option **EZ Setup** (Einfache Konfiguration) aus. Der folgende Bildschirm wird angezeigt:



2. Wählen Sie entweder **Yes** (Ja) oder **No, I want to configure the router myself** (Nein, ich möchte den Router selbst einrichten) aus. Wenn Sie **No** (Nein) wählen, fahren Sie mit *Internetkonfiguration (Grundeinstellungen)* auf Seite 20 fort.
3. Klicken Sie bei Auswahl von **Yes** (Ja) auf **Next** (Weiter).

   Bei automatischer Interneterkennung durchsucht der EZ Setup-Assistent die Internetverbindung nach Servern und Protokollen, um Ihre ISP-Konfiguration bestimmen zu können.

Hinweis: Der EZ Setup-Assistent kann keine Point-to-Point-Tunneling-Protocol-Verbindung (PPTP) erkennen. Falls Ihr ISP PPTP verwendet, müssen Sie Ihre Internetverbindung über den unter *Internetkonfiguration (Grundeinstellungen)* auf Seite 20 beschriebenen Bildschirm einrichten.

➢ **So beheben Sie Fehler bei einer nicht erfolgreichen Internetverbindung:**

1. Überprüfen Sie sämtliche Einstellungen, um sicherzustellen, dass Sie die richtigen Optionen gewählt und alles korrekt eingegeben haben.
2. Wenden Sie sich an Ihren Provider und vergewissern Sie sich, dass Ihnen die richtigen Konfigurationsdaten vorliegen.
3. Lesen Sie den Abschnitt *Kapitel 7, Fehlerbehebung*. Falls die Probleme weiterhin bestehen, registrieren Sie Ihr Produkt, und wenden Sie sich an den technischen Support.
4. Falls Sie keine Verbindung zum Router herstellen können, überprüfen Sie die Eigenschaften des Internetprotokolls (TCP/IP) der Netzwerkverbindung in der Systemsteuerung Ihres Computers. Stellen Sie dort sicher, dass Ihr Computer IP-Adresse *und* DNS-Server-Adresse automatisch bezieht. Weitere Informationen finden Sie in der Dokumentation Ihres Computers.

Herstellen einer Verbindung mit einem WLAN-Netzwerk

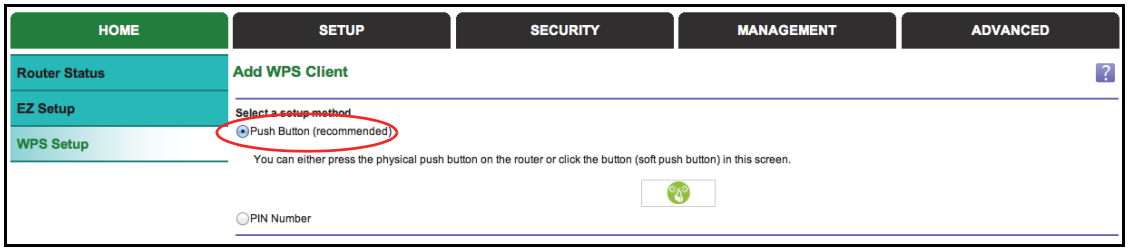
Wählen Sie entweder die WPS-Methode oder die manuelle Methode, um eine Verbindung mit dem WLAN-Netzwerk herzustellen.

WPS-Methode

Mit WPS (Wi-Fi Protected Setup) können Sie eine Verbindung mit einem sicheren WLAN-Netzwerk herstellen, ohne das Passwort einzugeben. Stattdessen drücken Sie eine Taste oder geben eine PIN ein. Einige ältere WLAN-Geräte sind nicht zu WPS kompatibel. WPS kann nur mit den Sicherheitsoptionen WPA2 oder WPA verwendet werden.

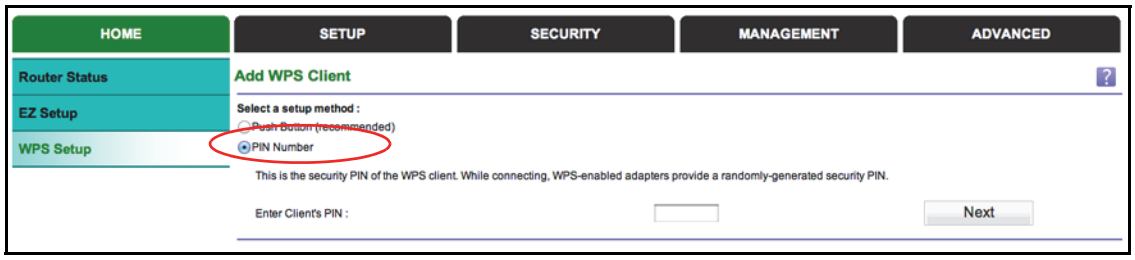
➢ **So verwenden Sie die WPS-Methode, wenn Sie am Router angemeldet sind:**

1. Wählen Sie **Home** (Start) > **WPS Setup** (WPS-Konfiguration).
2. Klicken Sie auf **Next** (Weiter). Auf dem folgenden Bildschirm können Sie die Methode zum Hinzufügen des WPS-Clients auswählen.



3. Wählen Sie **Push Button** (Tastendruck) oder **PIN Number** (PIN-Nummer) aus. Bei jeder der Methoden versucht der Router, mit dem Computer oder Gerät zu kommunizieren, die Wireless-Sicherheit für das Gerät einzurichten und ihm zu erlauben, sich mit dem Netzwerk zu verbinden.

4. Geben Sie die Sicherheits-PIN des Clients ein, wenn der Bildschirm für die PIN-Methode angezeigt wird.



Wenn der Router eine WPS-Verbindung herstellt, wird auf dem WPS-Bildschirm des Routers eine Bestätigungsmeldung angezeigt.

Manuelle Methode

Bei der manuellen Methode wählen Sie das gewünschte Netzwerk aus und geben das zugehörige Passwort ein, um eine Verbindung herzustellen.

➢ **So stellen Sie manuell eine Verbindung her:**

1. Starten Sie auf dem Computer oder Wireless-Gerät die Software, mit der die WLAN-Verbindungen verwaltet werden. Diese Software sucht nach allen verfügbaren Wireless-Netzwerken in Ihrer Umgebung.
2. Suchen Sie Ihr Netzwerk, und wählen Sie es aus.

   Der eindeutige WLAN-Netzwerkname (SSID) und das Password sind auf dem Typenschild des Routers angegeben. Wenn Sie diese Einstellungen geändert haben, suchen Sie den Netzwerknamen, den Sie verwendet haben.
3. Geben Sie das Router-Kennwort ein, und klicken Sie auf **Connect** (Verbinden).

3 Router-Konfiguration

Optionen auf der Registerkarte **Setup** (Konfiguration)

Dieses Kapitel enthält die folgenden Abschnitte:

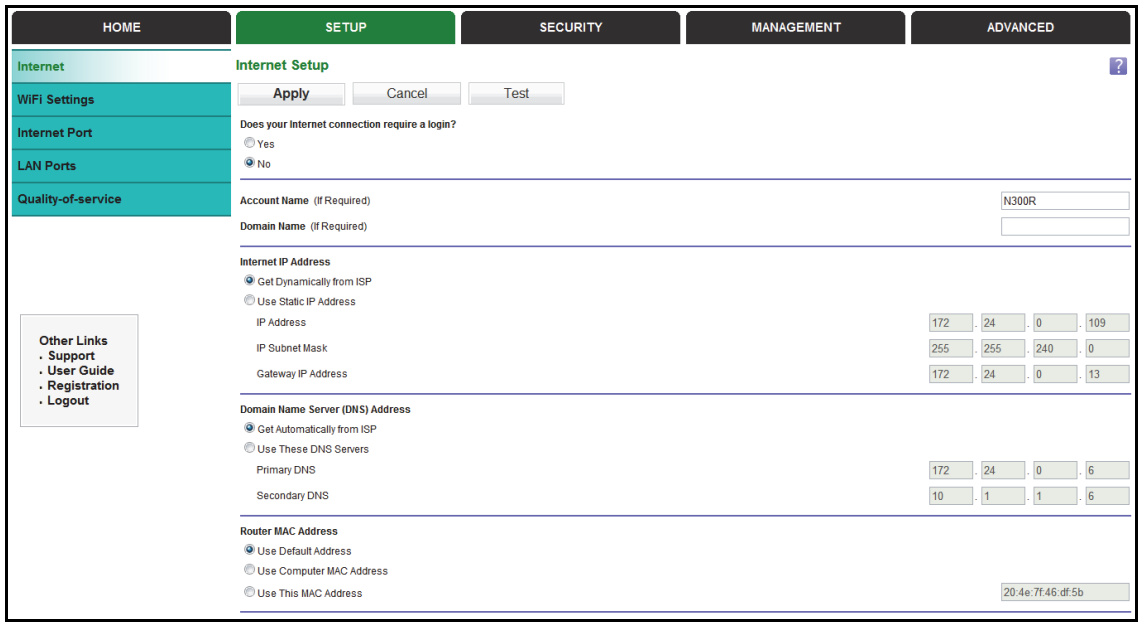
- *Internetkonfiguration (Grundeinstellungen)*
- *Voreingestellte Sicherheit*
- *Grundlagen der WLAN-Sicherheit*
- *WiFi-Setup*
- *Internet-Port*
- *LAN-Ports*
- *QoS (Quality of Service)-Konfiguration*

Internetkonfiguration (Grundeinstellungen)

Der Bildschirm **Basic Settings** (Grundeinstellungen) wird angezeigt, wenn Sie im Setup-Assistenten die Option **No, I want to configure the Router myself** (Nein, ich möchte den Router selbst einrichten) wählen. Er kann auch im Menü des Routers aufgerufen werden. Hier können Sie ISP-Informationen anzeigen und ändern. Je nachdem, ob Ihre Internetverbindung eine Anmeldung erfordert, werden unterschiedliche Felder angezeigt.

➢ **So konfigurieren Sie die Internetverbindung manuell:**

1. Wählen Sie **Setup** (Konfiguration) > **Internet**.



2. Wählen Sie abhängig davon, ob Ihr ISP eine Anmeldung erfordert, **Yes** (Ja) oder **No** (Nein).
   - **Yes** (Ja): Wählen Sie die Verkapselungsmethode aus, und geben Sie den Anmeldenamen ein. Wenn Sie die Zeitüberschreitung für die Anmeldung ändern möchten, geben Sie einen neuen Wert in Minuten ein.
   - **No** (Nein): Geben Sie den Konto- und Domainnamen ein (falls erforderlich).
3. Geben Sie die Einstellungen für die IP-Adresse und den DNS-Server ein. Normalerweise können Sie die DSL-Standardeinstellungen beibehalten. Falls Probleme bei der Verbindungsherstellung auftreten, überprüfen Sie die ISP-Einstellungen.
4. Falls keine Anmeldung erforderlich ist, können Sie die Einstellung der MAC-Adresse vornehmen.
5. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.
6. Klicken Sie auf **Test** (Testen), um die Internetverbindung zu testen. Wenn innerhalb einer Minute keine Verbindung hergestellt werden kann, lesen Sie die Informationen unter *Kapitel 7, Fehlerbehebung*.

In den folgenden Beschreibungen werden alle verfügbaren Felder auf dem Bildschirm **Basic Settings** (Grundeinstellungen) erläutert. Welche Felder auf diesem Bildschirm angezeigt werden, ist davon abhängig, ob eine Anmeldung beim ISP erforderlich ist.

Ist eine Anmeldung bei Ihrem ISP erforderlich? Antworten Sie mit **Yes** (Ja) oder **No** (Nein).

- *Ist keine Anmeldung erforderlich, werden diese Felder angezeigt*:

  Account Name (If required) (Kontoname [falls erforderlich]): Geben Sie den Kontonamen ein, den Sie von Ihrem ISP erhalten haben. Möglicherweise wird er auch als Hostname bezeichnet.

  Domain Name (If required) (Domainname [falls erforderlich]): Geben Sie den Domainnamen ein, den Sie von Ihrem ISP erhalten haben.

- *Erfordert Ihr ISP eine Anmeldung, so werden diese Felder angezeigt*:

  Internet Service Provider (Internet-Dienstanbieter): Verkapselung ist eine Methode zum Einschluss mehrerer Protokolle. PPP steht für Point-to-Point-Protokoll. Die Auswahlmöglichkeiten sind PPPoE (PPP over Ethernet) und PPPoA (PPP over ATM).

  Login (Anmeldung): Der Anmeldename, den Sie von Ihrem ISP erhalten haben. Dabei handelt es sich oft um eine E-Mail-Adresse.

  Password (Passwort): Das Passwort, mit dem Sie sich bei Ihrem ISP anmelden.

  Service Name (Dienstname), falls erforderlich.

  Connection Mode (Verbindungsmodus):

  Idle Timeout (In minutes) (Leerlaufzeit [in Minuten]): Wenn Sie die Zeitüberschreitung für die Anmeldung ändern möchten, geben Sie einen neuen Wert in Minuten ein. Dadurch wird festgelegt, wie lange der Router die Internetverbindung aktiv aufrecht erhält, nachdem die letzte Internetaktivität über das LAN verzeichnet wurde. Bei Eingabe des Werts 0 (null) werden Sie nie abgemeldet.

Internet IP Address (Internet-IP-Adresse)

- *Ist eine Anmeldung erforderlich, werden diese Felder angezeigt*:

  Get Dynamically from ISP (Dynamisch vom ISP beziehen): Der ISP verwendet DHCP, um Ihnen Ihre IP-Adresse zuzuweisen. Der ISP weist diese Adressen automatisch zu.

  Use Static IP-Address (Statische IP-Adresse verwenden): Geben Sie die IP-Adresse, IP-Subnetzmaske und Gateway-IP-Adresse ein, die Ihr ISP Ihnen zugewiesen hat. Das Gateway ist der Router des ISP, mit dem Ihr Router eine Verbindung herstellt.

- *Ist keine Anmeldung erforderlich, wird dieses Feld angezeigt*:

  Use IP Over ATM (IPoA) (IPoA (IP over ATM) verwenden): Ihr ISP verwendet klassische IP-Adressen (RFC 1577). Geben Sie die IP-Adresse, IP-Subnetzmaske und Gateway-IP-Adresse ein, die Ihr ISP Ihnen zugewiesen hat.

Domain Name Server (DNS) Address (DNS-Adresse [Domain Name Service]): Jedem Domainnamen im Internet ist eine IP-Nummer zugeordnet, die der Webbrowser zum Anzeigen der entsprechenden Websites benötigt und die er über einen DNS-Server (Domain Name Service) abruft.

- **Get Automatically from ISP** (Automatisch vom ISP beziehen): Der ISP verwendet DHCP, um Ihnen DNS-Server zuzuweisen. Der ISP weist diese Adresse automatisch zu.
- **Use These DNS Servers** (Diese DNS-Server verwenden): Wenn Sie wissen, dass Ihr ISP die DNS-Adressen während der Anmeldung nicht automatisch an den Router überträgt, wählen Sie diese Option aus, und geben Sie die IP-Adresse des primären DNS-Servers des ISPs ein. Falls außerdem die Adresse eines sekundären DNS-Servers bekannt ist, geben Sie diese ebenfalls ein.

MAC-Adresse des Routers: Die vom Router verwendete Netzwerk-MAC-Adresse für den Internet-Port. Einige ISPs registrieren die MAC-Adresse der Netzwerkkarte bei der Einrichtung des Kontos auf dem Computer. Danach akzeptieren sie nur Datenverkehr von der MAC-Adresse dieses Computers. Diese Funktion ermöglicht dem Router die Verwendung der MAC-Adresse Ihres Computers. (Dies wird auch als Klonen bezeichnet.)

- **Use Default Address** (Standardadresse verwenden): Die Standard-MAC-Adresse wird verwendet.
- **Use Computer MAC Address** (MAC-Adresse des Computers verwenden): Der Router erfasst und verwendet die MAC-Adresse des aktuell verwendeten Computers. Verwenden Sie also den Computer, der beim ISP zugelassen ist.
- **Use This MAC Address** (Diese MAC-Adresse verwenden): Geben Sie die MAC-Adresse ein, die verwendet werden soll.

Voreingestellte Sicherheit

Der Router verfügt über voreingestellte Sicherheitsfunktionen. Dies bedeutet, dass der WLAN-Netzwerkname (SSID), die Passphrase und die Sicherheitsoption (Verschlüsselungsprotokoll) bereits vor der Auslieferung eingestellt werden. Die voreingestellte SSID und die voreingestellte Passphrase befinden sich an der Unterseite des Geräts.

- **Wi-Fi network name (SSID)** (WLAN-Netzwerkname [SSID]) bezeichnet Ihr Netzwerk, sodass es von Geräten gefunden werden kann.
- **Passphrase** steuert den Zugriff auf Ihr Netzwerk. Geräte, denen SSID und Passphrase bekannt sind, können Ihr WLAN-Netzwerk finden und eine Verbindung damit herstellen.
- **Security option** (Sicherheitsoption) bezeichnet die Art des Sicherheitsprotokolls für das WLAN. Mit dem angewendeten Sicherheitsprotokoll wird die Datenübertragung verschlüsselt, und es wird sichergestellt, dass nur vertrauenswürdige Geräte eine Autorisierung zur Verbindung mit dem Netzwerk erhalten. Bei der Option zur Sicherheitsvoreinstellung handelt es sich um den gemischten Modus aus WPA-PSK/WPA2-PSK, siehe *WLAN-Sicherheitsoptionen* auf Seite 24.

Auf dem Bildschirm **Wireless Settings** (WLAN-Konfiguration) können Sie die voreingestellten Sicherheitseinstellungen anzeigen und bearbeiten. ***Es empfiehlt sich jedoch, die voreingestellten Sicherheitseinstellungen zu verwenden.*** Wenn Sie die voreingestellten Sicherheitseinstellungen dennoch ändern, notieren Sie die neuen Einstellungen, und bewahren Sie sie an einem sicheren Ort auf, an dem Sie sie problemlos wieder finden.

Grundlagen der WLAN-Sicherheit

Anders als bei kabelgebundenen Netzwerken können drahtlos übertragene Daten auch von außerhalb mit jedem beliebigen Gerät empfangen werden, das über einen kompatiblen Wireless-Adapter (Funkgerät) verfügt. Daher ist es sehr wichtig, dass Sie die voreingestellten Sicherheitseinstellungen beibehalten und die anderen verfügbaren Sicherheitsfunktionen verstehen. Abgesehen von den im vorigen Abschnitt beschriebenen voreingestellten Sicherheitseinstellungen verfügt Ihr Router über die hier und in *Kapitel 4, Sicherheitseinstellungen* beschriebenen Sicherheitsfunktionen.

- Wireless-Verbindung abschalten
- SSID-Broadcast deaktivieren
- Einschränkung des Zugriffs über MAC-Adressen
- Wireless-Sicherheitsoptionen

Deaktivieren des SSID-Broadcast

Standardmäßig sendet der Router seinen WLAN-Netzwerknamen (SSID), sodass er von Geräten gefunden werden kann. Wenn Sie diese Einstellung ändern, sodass das Versenden nicht zugelassen wird, können Wireless-Geräte Ihren Router erst finden, wenn sie mit der gleichen SSID konfiguriert werden.

Hinweis: Durch das Abschalten von SSID-Broadcast wird die „Entdeckungsfunktion“ für WLAN-Netzwerke von Produkten wie Windows XP außer Betrieb gesetzt, doch die Daten sind immer noch ungeschützt gegen hartnäckige Schnüffler, die spezielle Software wie Wireless Sniffer einsetzen. Wenn Sie das Versenden zulassen, stellen Sie sicher, dass die Wireless-Sicherheit aktiviert ist.

Einschränkung des Zugriffs über MAC-Adressen

Sie können Ihre Netzwerksicherheit erhöhen, indem Sie den Zugriff nur für bestimmte PCs anhand ihrer MAC-Adressen (Media Access Control) zulassen. Sie können den Zugang auf bekannte PCs beschränken, damit unbekannte PCs keine Wireless-Verbindung zum Router aufbauen können. Die Filterung der MAC-Adressen der WLAN-Geräte fügt der bereits aktivierten Wireless-Sicherheitsoption noch zusätzlichen Schutz hinzu. Die Liste der zugriffsberechtigten Geräte legt anhand der MAC-Adressen fest, welche Wireless-Hardwaregeräte mit dem Router in Verbindung treten dürfen. Die entsprechende Vorgehensweise finden Sie unter *Erweiterte WLAN-Konfiguration* auf Seite 68.

WLAN-Sicherheitsoptionen

Eine Sicherheitsoption bezeichnet die Art des Sicherheitsprotokolls für das WLAN. Mit dem Sicherheitsprotokoll wird die Datenübertragung verschlüsselt, und es wird sichergestellt, dass nur vertrauenswürdige Geräte eine Autorisierung zur Verbindung mit dem Netzwerk erhalten. Es gibt diverse Verschlüsselungsmethoden: Wi-Fi Protected Access II (WPA2), WPA und Wired Equivalent Privacy (WEP). WPA2 ist die neueste und sicherste Methode und wird empfohlen, sofern Ihre Geräte sie unterstützen. WPA verfügt über mehrere Optionen, z. B. PSK-Verschlüsselung (Pre-Shared Key) und 802.1x-Verschlüsselung für Unternehmen. Die WLAN-Sicherheitseinstellungen können deaktiviert werden, dies wird jedoch nicht empfohlen. Sie können die WLAN-Sicherheitsoptionen im Bildschirm **Wireless Settings** (WLAN-Konfiguration) anzeigen und bearbeiten. Siehe *WiFi-Setup* auf Seite 24.

WiFi-Setup

Im Bildschirm **Wireless Settings** (WLAN-Konfiguration) können Sie die Einstellungen des WLAN-Netzwerks anzeigen oder konfigurieren. Ihr voreingestellter Router verfügt über einen eindeutigen Netzwerknamen und ein eindeutiges Passwort. Diese befinden sich auf dem Typenschild. Es empfiehlt sich, diese Einstellungen zu verwenden. Falls Sie sich entschließen, sie zu ändern, notieren Sie bitte die neuen Einstellungen, und bewahren Sie sie an einem sicheren Ort auf.

Hinweis: Wenn Sie einen WLAN-Computer zur Änderung des WLAN-Netzwerknamens (SSID) oder anderer Sicherheitsoptionen verwenden, wird die Verbindung getrennt, wenn Sie auf **Apply** (Übernehmen) klicken. Verwenden Sie einen Computer mit Kabelverbindung für den Zugriff auf den Router, um dieses Problem zu umgehen.

Überprüfen jedes Geräts in Ihrem Netzwerk

Überprüfen Sie Folgendes, bevor Sie beginnen:

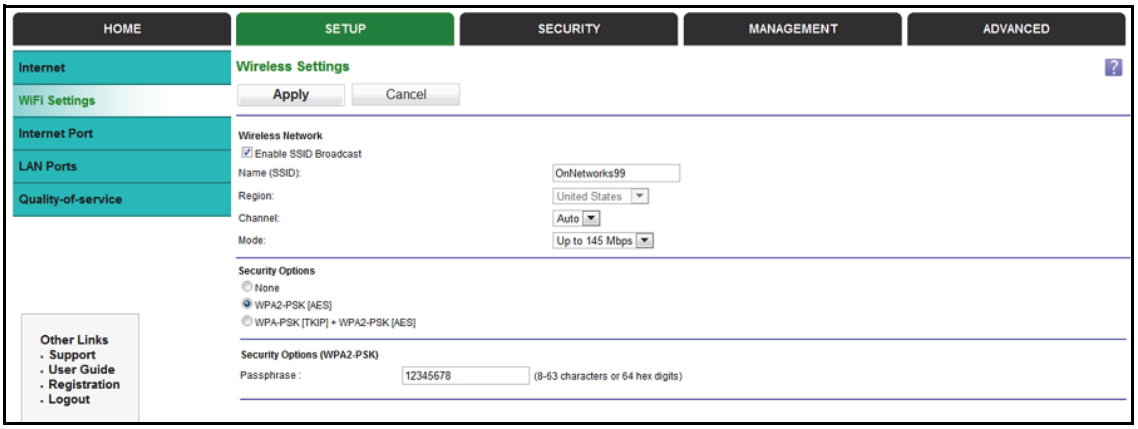
- Jeder WLAN-Computer muss in der Lage sein, eine IP-Adresse über DHCP vom Router zu beziehen, wie in *Verwenden der Standard-TCP/IP-Eigenschaften für DHCP* auf Seite 12 beschrieben.
- Jeder Computer oder Wireless-Adapter in Ihrem Netzwerk muss die gleiche SSID und den gleichen WLAN-Modus (Bandbreite/Übertragungsrate) aufweisen wie der Router. Überprüfen Sie, ob die Wireless-Adapter der einzelnen Computer die von Ihnen ausgewählten Modus- und Sicherheitsoptionen unterstützen.
- Die Sicherheitsoption auf jedem Wireless-Gerät im Netzwerk muss zumRouter passen. Wenn Sie beispielsweise eine Sicherheitsoption wählen, die eine Passphrase erfordert, verwenden Sie bitte unbedingt die gleiche Passphrase für jeden WLAN-Computer im Netzwerk.

Anzeigen oder Ändern der WLAN-Konfiguration

Ihr voreingestellter Router wird mit einem eindeutigen WLAN-Netzwerknamen (SSID) und einem eindeutigen Netzwerkpasswort geliefert. Diese Informationen sind auf das Typenschild Ihres Routers aufgedruckt. Sie können diese Einstellungen mithilfe des Bildschirms **Wireless Settings** (WLAN-Konfiguration) anzeigen und bearbeiten.

➢ **So zeigen Sie die WLAN-Konfiguration an oder ändern sie:**

1. Wählen Sie **Setup** (Konfiguration) > **WiFi Settings** (WLAN-Konfiguration). Der folgende Bildschirm wird angezeigt.



2. Nehmen Sie alle erforderlichen Änderungen vor, und klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Hinweis: Die Abschnitte, Einstellungen und Vorgehensweisen dieses Bildschirms werden im Folgenden erläutert.

3. Konfigurieren und testen Sie die Wireless-Verbindung Ihrer Computer.
   a. Verwenden Sie Ihren Wireless-Computer bzw. Ihr Wireless-Gerät, um eine Verbindung mit dem Netzwerk herzustellen. Geben Sie bei Aufforderung das Netzwerkpasswort ein.
   b. Stellen Sie bei einem drahtlos verbundenen Computer sicher, dass Sie auf das Internet zugreifen können.

Felder auf dem Bildschirm **Wireless Settings** (WLAN-Konfiguration)

- **Enable SSID Broadcast** (SSID-Broadcast aktivieren): Diese Einstellung ermöglicht die Übertragung der SSID des Routers, damit WLAN-Geräte diesen WLAN-Namen (SSID) in ihrer Liste der gescannten Netzwerke anzeigen können. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen **Allow Broadcast of Name (SSID)** (SSID-Broadcast aktivieren), und klicken Sie auf **Apply** (Übernehmen), um die SSID-Übertragung zu deaktivieren.

- **Name (SSID)** (Netzwerkname [SSID]): Die SSID wird auch als Netzwerkname bezeichnet. Geben Sie einen (maximal) 32 Zeichen langen Namen in dieses Feld ein. Bei diesem Feld wird zwischen Groß- und Kleinschreibung unterschieden. Die standardmäßige SSID wird nach dem Zufallsprinzip generiert und muss normalerweise nicht geändert werden.
- **Region**: Der Ort, an dem der Router verwendet wird. Wenn Sie den Router in einer anderen Region als den hier aufgelisteten betreiben, verstoßen Sie möglicherweise gegen gesetzliche Bestimmungen.
- **Channel** (Kanal): Der Funkkanal, der von Gateway 1 bis 13 verwendet wird. Ändern Sie den Kanal nicht, es sei denn, es treten Funkstörungen auf (was sich durch abgebrochene Verbindungen und/oder langsame Datenübertragung zeigt). Testen Sie in diesem Fall verschiedene Kanäle, um den optimalen Kanal zu finden.
- **Mode** (Modus): Die Standardeinstellung **Up to 150 Mbps** (Bis zu 150 MBit/s) ermöglicht WLAN-Geräten der Standards 802.11n und 802.11g die Verbindung mit dem Netzwerk. g und b unterstützen bis zu 54 MBit/s.

Konfiguration der Sicherheitsoptionen

Im Abschnitt **Security Options** (Sicherheitsoptionen) auf dem Bildschirm **Wireless Settings** (WLAN-Konfiguration) können Sie die Sicherheitsoption und die Passphrase ändern. Auf dem Router sind bereits WPA2 und WPA konfiguriert. Weitere Informationen zum Ändern dieser Einstellungen finden Sie im folgenden Abschnitt, *Ändern der WPA-Sicherheitsoption und Passphrase*.

Ändern der WPA-Sicherheitsoption und Passphrase

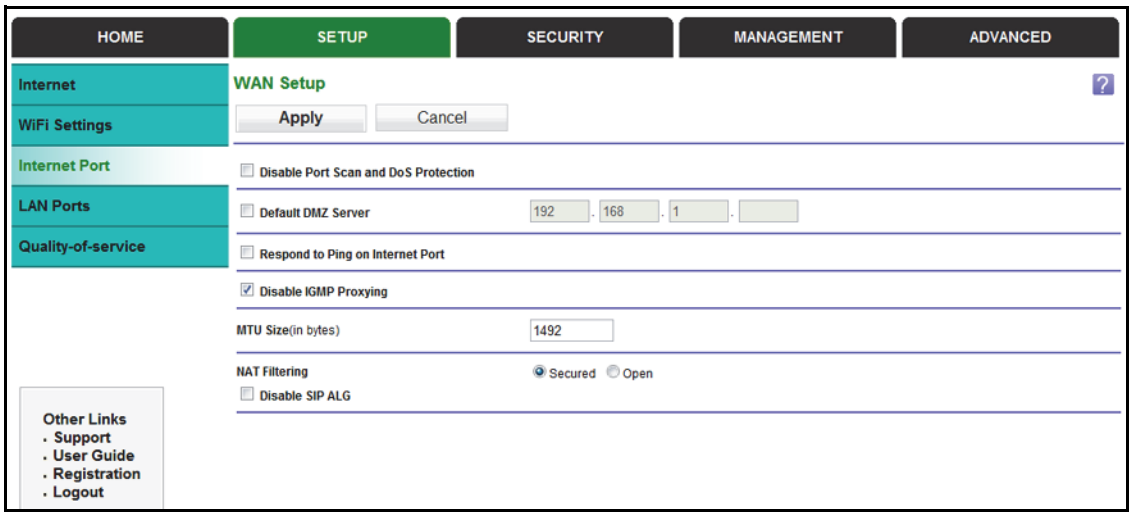
➢ **So ändern Sie die WPA-Sicherheitsoption:**

1. Wählen Sie im Abschnitt **Security options** (Sicherheitsoptionen) die gewünschte WPA-Option.

2. Geben Sie die Passphrase ein, die verwendet werden soll. Dabei handelt es sich um eine Textzeichenfolge mit einer Länge von 8 bis 63 Zeichen.
3. Klicken Sie auf **Apply** (Übernehmen).

Internet-Port

Mit dem Bildschirm **WAN Setup** (WAN-Konfiguration) können Sie einen DMZ-Server (Demilitarized Zone; entmilitarisierte Zone) konfigurieren, die MTU-Größe (Maximum Transmit Unit) ändern und den Router so einrichten, dass er auf Ping-Anforderungen am WAN (Internet)-Port reagiert. Wählen Sie **Setup** (Konfiguration) > **Internet Port** (Internet-Port) aus. Der folgende Bildschirm wird geöffnet:



- **Disable Port Scan and DoS Protection** (Schutz vor Port-Abfragen und DoS-Angriffen deaktivieren): Der Schutz vor DoS schützt Ihr LAN vor Denial of Service-Angriffen wie SYN-Floods, Smurf-Angriffen, Ping of Death, Teardrop-Angriffen, UDP-Floods, ARP-Angriffen, Spoofing (ICMP), Null-Scans u. a. Diese Option sollte nur deaktiviert werden, wenn dies aus gegebenem Anlass erforderlich ist.
- **Default DMZ Server** (DMZ-Standardserver): Diese Funktion kann beim Spielen von Online-Spielen oder bei Videokonferenzen hilfreich sein. Seien Sie vorsichtig bei Verwendung dieser Funktion, da die Firewall-Sicherheitseinstellungen dadurch weniger effektiv sind. Weitere Informationen finden Sie im folgenden Abschnitt, *DMZ-Standardserver*.
- **Respond to Ping on Internet Port** (Auf Ping-Anforderungen am Internet-Port reagieren): Aktivieren Sie dieses Kontrollkästchen, wenn der Router auf Ping-Anforderungen aus dem Internet reagieren soll. Diese Option sollte nur für Diagnosezwecke verwendet werden, da Ihr Router dadurch entdeckt werden kann. Aktivieren Sie dieses Kästchen nur, wenn ein dringender Grund dazu vorliegt.
- **Disable IGMP Proxying (**IGMP-Proxy deaktivieren): Die IGMP-Proxyfunktion ermöglicht es einem Computer im LAN (Local Area Network), den gewünschten Multicast-Datenverkehr aus dem Internet zu empfangen. Sie können das Kontrollkästchen aktivieren und die Funktion damit deaktivieren, wenn Sie sie nicht benötigen.
- **MTU Size (in bytes)** (MTU-Größe [in Byte]): Der MTU-Wert (Maximum Transmit Unit) beträgt normalerweise 1.500 Byte für lokale Netzwerke und 1.492 Byte für PPPoE-Verbindungen. Bei einigen ISPs muss ein niedrigerer MTU-Wert eingestellt werden. Dies ist nur selten erforderlich. Reduzieren Sie den MTU-Wert nur, wenn dies für Ihre ISP-Verbindung tatsächlich erforderlich ist. Siehe *Ändern der MTU-Größe* auf Seite 28.

- **NAT Filtering** (NAT-Filter): NAT (Network Address Translation) legt fest, wie eingehender Datenverkehr vom Router verarbeitet wird. Bei Auswahl der Option für sicheres NAT werden die Computer im LAN durch eine sichere Firewall vor Angriffen aus dem Internet geschützt. Allerdings kann dies dazu führen, dass einige Online-Spiele, Point-to-Point-Anwendungen und Multimedia-Anwendungen nicht funktionieren. Bei Auswahl der Option für offenes NAT ist die Firewall nicht so sicher, es können jedoch fast alle Internetanwendungen ausgeführt werden.

DMZ-Standardserver

Der DMZ-Standardserver kann bei Online-Spielen und Videokonferenz-Anwendungen, die nicht zu NAT (Network Address Translation) kompatibel sind, hilfreich sein. Der Router ist darauf programmiert, einige dieser Anwendungen zu erkennen und zu unterstützen, doch bei anderen Anwendungen können Probleme auftreten. In einigen Fällen ist es möglich, die Anwendung auf einem lokalen Computer fehlerfrei auszuführen, wenn die IP-Adresse des Computers als DMZ-Standardserver eingegeben wird.

WARNUNG:

DMZ-Server stellen ein Sicherheitsrisiko dar. Ein Computer, der als DMZ-Standardserver festgelegt wird, verliert einen Großteil des Firewall-Schutzes und ist Angriffen aus dem Internet ausgesetzt. Dies kann dazu führen, dass der DMZ-Server-Computer für Angriffe auf andere Computer in Ihrem Netzwerk verwendet wird.

Über das Internet eingehende Daten werden normalerweise vom Router zurückgewiesen, wenn sie nicht von einem Ihrer lokalen Computer angefordert wurden oder zu einem der im Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) konfigurierten Dienste gehören. Statt diese Daten zurückzuweisen, können Sie sie vom Router an einen Computer in Ihrem Netzwerk weiterleiten. Dieser Computer ist der DMZ-Standardserver.

➢ **So richten Sie einen DMZ-Standardserver ein:**

1. Aktivieren Sie auf dem Bildschirm **Internet Port** (Internet-Port) das Kontrollkästchen **Default DMZ Server** (DMZ-Standardserver).
2. Geben Sie die IP-Adresse ein.
3. Klicken Sie auf **Apply** (Übernehmen).

Ändern der MTU-Größe

Die MTU (Maximum Transmission Unit) ist das größte Datenpaket, das in einem Netzwerk übertragen wird. Wenn ein Netzwerkgerät über das Internet mit einem anderen Netzwerkgerät Daten austauscht, wandert das Datenpaket dabei über viele Geräte. Weist eines der Geräte im Datenpfad eine niedrigere MTU-Einstellung als die anderen Geräte auf, müssen die Datenpakete aufgeteilt oder „fragmentiert“ werden, damit auch das Gerät mit dem niedrigsten MTU-Wert die Daten weitersenden kann.

Die beste MTU-Einstellung für On Networks-Geräte ist oft die Standardeinstellung. Durch eine Änderung des Werts wird manchmal nur ein Problem behoben und dafür ein zusätzliches Problem geschaffen. Ändern Sie die MTU nur, wenn eine der folgenden Situationen eintritt:

- Sie können keine Verbindung mit Ihrem ISP oder einem anderen Internetdienst herstellen, und der technische Support des ISP oder On Networks empfiehlt eine Änderung der MTU-Einstellung. Für folgende webbasierte Anwendungen muss die MTU möglicherweise geändert werden:
  - Eine sichere Website, die nicht geöffnet werden kann oder eine Webseite nur zum Teil anzeigt
  - Yahoo!-E-Mail
  - MSN-Portal
  - DSL-Dienst von AOL
- Sie verwenden VPN und haben mit erheblichen Leistungsproblemen zu kämpfen.
- Sie haben zur Erhöhung der Leistung ein Programm für die MTU-Optimierung eingesetzt und haben nun Probleme mit der Verbindung oder Leistung.

Hinweis: Eine falsche MTU-Einstellung kann Probleme mit der Internetverbindung verursachen. Sie kann beispielsweise zur Folge haben, dass bestimmte Webseiten, Frames in Webseiten, sichere Anmeldeseiten oder FTP- oder POP-Server nicht mehr aufgerufen werden können.

Wenn Sie ein MTU-Problem vermuten, kann es häufig dadurch gelöst werden, die MTU zu 1400 zu ändern. Falls Sie verschiedene Lösungen ausprobieren möchten, können Sie die MTU nach und nach vom Maximalwert 1500 heruntersetzen, bis das Problem behoben ist. In der folgenden Tabelle werden häufige MTU-Größen und Anwendungen dargestellt.

Tabelle 2. Häufige MTU-Größen

MTU	Anwendung
1500	Die größte Netzwerkpaketgröße und der Standardwert. Dies ist die normale Einstellung für Verbindungen ohne PPPoE und VPN sowie der Standardwert für Router, Adapter und Switches von On Networks.
1492	Wird in PPPoE-Umgebungen verwendet
1472	Maximal verwendbare Größe für Ping-Anforderungen (Größere Pakete werden fragmentiert.)
1468	Wird in einigen DHCP-Umgebungen verwendet
1460	Verwendbar u. a. für AOL, wenn Sie keine großen E-Mail-Anhänge senden oder empfangen
1436	Wird in PPTP-Umgebungen oder mit VPN verwendet
1400	Maximale Größe für AOL-DSL
576	Normaler Wert für DFÜ-Verbindungen

➢ **So ändern Sie die MTU-Größe:**

1. Wählen Sie **Advanced** (Erweitert) > **Setup** (Konfiguration) > **WAN Setup** (WAN-Konfiguration) aus.
2. Geben Sie in das Feld **MTU Size** (MTU-Größe) einen Wert zwischen 64 und 1500 ein.
3. Klicken Sie auf **Übernehmen** (Apply), um die Einstellungen zu speichern.

LAN-Ports

Der Bildschirm **LAN Ports** (LAN-Ports) ermöglicht die Konfiguration von LAN-IP-Diensten wie DHCP (Dynamic Host Configuration Protocol) und RIP (Routing Information Protocol).

Der Router wird mit einer Voreinstellung zur Verwendung privater IP-Adressen im LAN und für die Verwendung als DHCP-Server ausgeliefert. Die voreingestellte LAN-IP-Konfiguration des Routers sieht wie folgt aus:

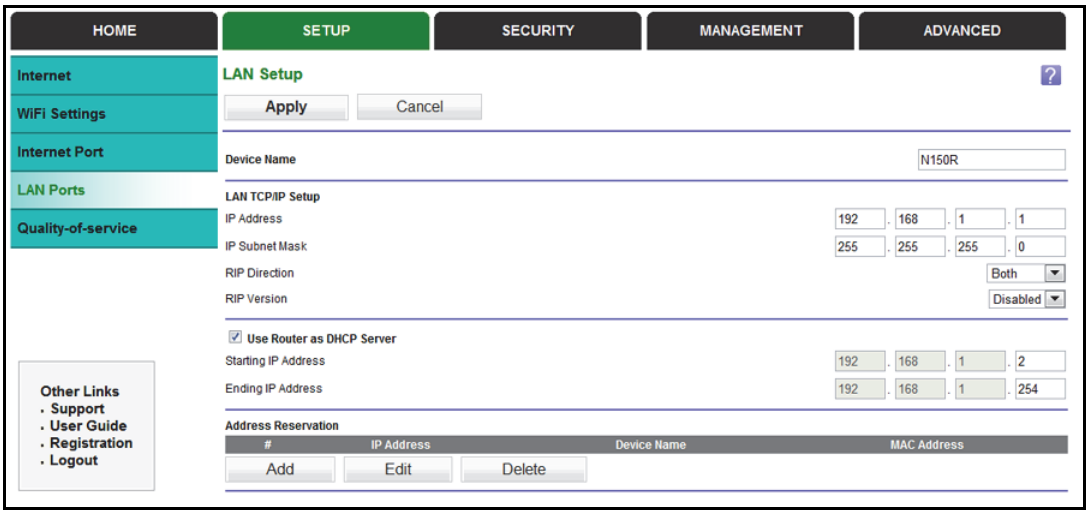
- LAN-IP-Adresse. **192.168.1.1**
- Subnetzmaske. **255.255.255.0**

Diese Adressen gehören zu dem für die Verwendung in privaten Netzwerken bestimmten privaten Adressbereich und sind für die meisten Anwendungen geeignet. Wenn für Ihr Netzwerk ein anderes IP-Adressenschema erforderlich ist, können Sie die entsprechenden Einstellungen auf dem Bildschirm **LAN Setup** (LAN-Konfiguration) vornehmen.

➢ **So ändern Sie die LAN-Einstellungen:**

Hinweis: Wenn Sie die LAN-IP-Adresse des Routers ändern, während Sie über den Browser verbunden sind, wird die Verbindung unterbrochen. Sie müssen dann eine Verbindung zur neuen IP-Adresse herstellen und sich erneut anmelden.

1. Wählen Sie **Setup** (Konfiguration) > **LAN Setup** (LAN-Konfiguration) aus, um den folgenden Bildschirm anzuzeigen:



2. Geben Sie die Einstellungen ein, die Sie anpassen möchten. Diese Einstellungen werden im folgenden Abschnitt, *LAN-TCP/IP-Konfiguration*, beschrieben.
3. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

LAN-TCP/IP-Konfiguration

- **IP Address** (IP-Adresse): Die LAN-IP-Adresse des Routers
- **IP Subnet Mask** (IP-Subnetzmaske): Die LAN-Subnetzmaske des Routers. Zusammen mit der IP-Adresse sorgt die IP-Subnetzmaske dafür, dass ein Gerät erkennen kann, bei welchen Adressen es sich um lokale Adressen handelt und welche Adressen nur über ein Gateway oder einen Router zu erreichen sind.
- **RIP Direction** (RIP-Richtung): Über RIP (Router Information Protocol) kann ein Router Routinginformationen mit anderen Routern austauschen. Diese Einstellung legt fest, auf welche Weise der Router RIP-Pakete sendet und empfängt. Die Standardeinstellung ist **Both** (Beide). Bei Auswahl von **Both** (Beide) oder **Out Only** (Nur abgehend) sendet der Router die Routingtabelle in regelmäßigen Abständen. Bei Auswahl von **Both** (Beide) oder **In Only** (Nur ankommend) übernimmt der Router eingehende Routinginformationen.
- **RIP Version** (RIP-Version): Mit dieser Einstellung können Sie das Format und die Broadcastmethode für den Versand von RIP-Paketen durch den Router steuern. Beim Empfang werden beide Formate erkannt. Standardmäßig ist die RIP-Funktion deaktiviert.

  RIP-1 wird praktisch von allen Netzwerkgeräten unterstützt. Es eignet sich für alle gängigen Netzwerkkonfigurationen.

  Bei **RIP-2** werden mehr Informationen übertragen. Sowohl bei RIP-2B als auch bei RIP-2M werden die Routingdaten im RIP-2-Format übermittelt. Bei RIP-2B erfolgt die Übertragung mittels Subnetz-Broadcasting. Bei RIP-2M erfolgt die Übertragung mittels Multicasting.

Use Router as a DHCP Server *(Router als DHCP-Server verwenden)*

Dieses Kontrollkästchen ist standardmäßig aktiviert, damit der Router als DHCP-Server (Dynamic Host Configuration Protocol) verwendet wird.

- **Starting IP Address** (Erste IP-Adresse): Geben Sie den Beginn des Bereichs für den IP-Adresspool im Subnetz des Routers an.
- **Ending IP Address** (Letzte IP-Adresse): Geben Sie das Ende des Bereichs für den IP-Adresspool im Subnetz des Routers an.

Adressreservierung

Wenn Sie für einen Computer im LAN eine reservierte IP-Adresse angeben, wird diesem Computer bei jedem Zugriff auf den DHCP-Server des Routers dieselbe IP-Adresse zugewiesen. Weisen Sie Servern, die feste IP-Einstellungen erfordern, reservierte IP-Adressen zu.

Verwenden des Routers als DHCP-Server

Standardmäßig fungiert der Router als DHCP-Server. Der Router vergibt IP-, DNS-Server- und Standardgateway-Adressen an alle Computer, die mit dem LAN verbunden sind. Als Standardgateway-Adresse wird die LAN-Adresse des Routers vergeben. Der Router vergibt IP-Adressen an die angeschlossenen Computer aus einer Auswahl von IP-Adressen, die auf diesem Bildschirm festgelegt werden. Jede dieser Adressen wird vor der Vergabe getestet, um doppelte Adressen im LAN zu verhindern. Für die meisten Anwendungen genügen die DHCP- und TCP/IP-Voreinstellungen des Routers.

Sie können die IP-Adressen angeben, die zur Vergabe verfügbar sein sollen, indem Sie die erste und letzte IP-Adresse festlegen. Diese Adressen sollten zum selben IP-Adressen-Subnetz gehören wie die LAN-IP-Adresse des Routers. Wenn Sie das Standard-Adressenschema verwenden, legen Sie einen Bereich zwischen 192.168.1.2 und 192.168.1.254 fest. Halten Sie jedoch ggf. einen Teil des Bereichs für Geräte mit festen IP-Adressen frei.

Der Router übermittelt die folgenden Parameter an jedes LAN-Gerät, das eine DHCP-Anforderung absendet:

- Eine IP-Adresse aus dem festgelegten Bereich
- Subnetzmaske
- Gateway-IP-Adresse (die LAN-IP-Adresse des Routers)
- Primärer DNS-Server (wenn Sie auf dem Bildschirm **Internet Setup** [Internetkonfiguration] eine primäre DNS-Adresse eingegeben haben – andernfalls die LAN-IP-Adresse des Routers)
- Sekundärer DNS-Server (wenn Sie auf dem Bildschirm **Internet Setup** [Internetkonfiguration] eine sekundäre DNS-Adresse eingegeben haben)

Wenn ein anderes Gerät in Ihrem Netzwerk als DHCP-Server eingesetzt werden soll oder Sie die Netzwerkeinstellungen auf allen Computern konfigurieren möchten, deaktivieren Sie das Kontrollkästchen **Use Router as DHCP Server** (Router als DHCP-Server verwenden), und klicken Sie auf **Apply** (Übernehmen). Lassen Sie dieses Kontrollkästchen andernfalls aktiviert. Wenn dieser Dienst nicht aktiviert ist und kein anderer DHCP-Server im Netzwerk verfügbar ist, müssen Sie die IP-Adressen der Computer manuell festlegen, da Sie sonst nicht auf den Router zugreifen können.

Adressreservierung

Wenn Sie für einen Computer im LAN eine reservierte IP-Adresse angeben, wird diesem Computer bei jedem Zugriff auf den DHCP-Server des Routers dieselbe IP-Adresse zugewiesen. Weisen Sie Computern oder Servern, die feste IP-Einstellungen erfordern, reservierte IP-Adressen zu.

- **So reservieren Sie eine IP-Adresse:**

1. Klicken Sie im Abschnitt **Address Reservation** (Adressreservierung) des Bildschirms auf die Schaltfläche **Add** (Hinzufügen).
2. Geben Sie im Feld IP Address (IP-Adresse) die IP-Adresse ein, die dem Computer oder Server zugewiesen werden soll. (Wählen Sie eine IP-Adresse aus dem LAN-Subnetz des Routers aus, z. B. 192.168.1.x.)
3. Geben Sie die MAC-Adresse des Computers oder Servers ein.

   Tipp: Wenn der Computer bereits in Ihrem Netzwerk registriert ist, können Sie seine MAC-Adresse aus dem Bildschirm **Attached Devices** (Angeschlossene Geräte) kopieren und hier einfügen.

4. Klicken Sie auf **Apply** (Übernehmen), um die reservierte Adresse in die Tabelle aufzunehmen.

   Die reservierte Adresse wird erst zugewiesen, wenn der Computer das nächste Mal mit dem DHCP-Server des Routers Kontakt aufnimmt. Starten Sie den Computer neu, oder greifen Sie auf seine IP-Konfiguration zu, und erzwingen Sie eine DHCP-Freigabe und -Erneuerung.

Um den Eintrag einer reservierten Adresse zu bearbeiten oder zu löschen, wählen Sie die Optionsschaltfläche neben der reservierten Adresse aus, die Sie bearbeiten oder löschen möchten. Klicken Sie dann auf **Edit** (Bearbeiten) oder **Delete** (Löschen).

QoS (Quality of Service)-Konfiguration

QoS ist eine erweiterte Funktion, mit der Prioritäten für verschiedene Datentypen festgelegt werden können. Der N150R-Router unterstützt QoS-Prioritätseinstellungen über das WLAN und für die Internetverbindung. Sie können QoS im Bildschirm QoS Setup (QoS-Konfiguration) einrichten.

Wählen Sie **Setup** (Konfiguration) > **Quality of Service** aus, um den folgenden Bildschirm anzuzeigen:

Aktivieren von WMM QoS für drahtlose Multimedia-Anwendungen

Der N150R-Router unterstützt WMM QoS (Wi-Fi Multimedia Quality of Service), um dem drahtlosen Sprach- und Videodatenverkehr über das WLAN Priorität einzuräumen. Mit WMM QoS erhalten drahtlose Datenpakete Priorität vor anderen Anwendungen. Die vier Zugriffskriterien lauten Sprache, Video, bester Versuch und Hintergrund. Damit eine Anwendung die Vorteile von WMM QoS nutzen kann, muss sowohl für die Anwendung als auch für den Client, auf dem die Anwendung ausgeführt wird, WMM aktiviert sein. Ältere Anwendungen, die WMM nicht unterstützen, und Anwendungen, für die QoS nicht erforderlich ist, werden der Kategorie bester Versuch zugeordnet. Diese Kategorie steht in der Prioritätsliste nach Sprache und Video.

WMM QoS ist standardmäßig aktiviert. Sie können die Option im Bildschirm **QoS Setup** (QoS-Konfiguration) deaktivieren, indem Sie das Kontrollkästchen **Enable WMM** (WMM aktivieren) deaktivieren und auf **Apply** (Übernehmen) klicken.

Konfigurieren von QoS für den Internetzugriff

Sie können den folgenden Datenverkehrstypen Vorrang beim Internetzugriff einräumen:

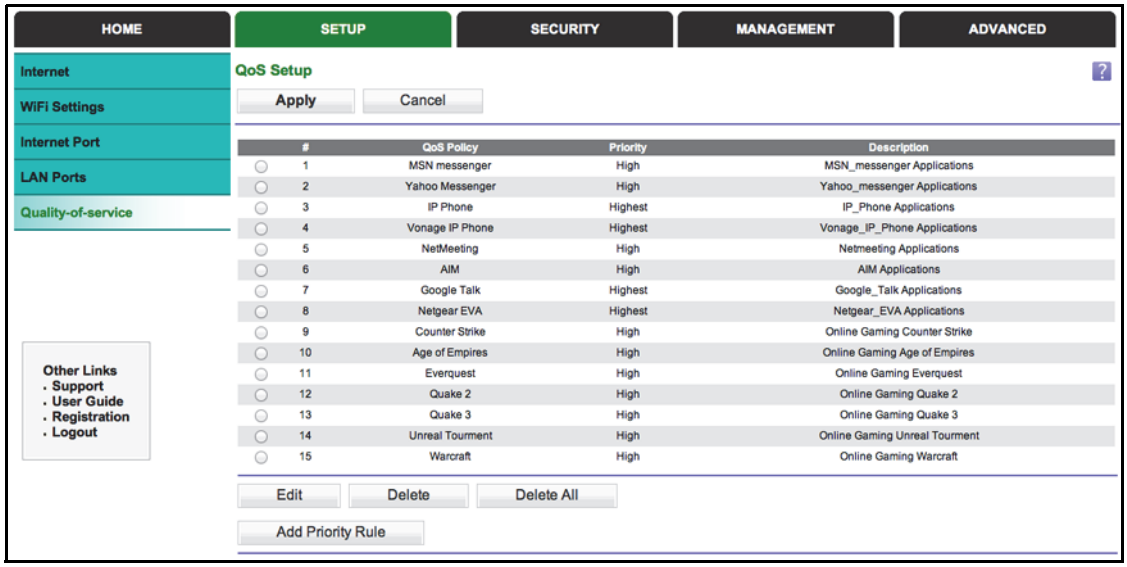
- Bestimmte Anwendungen
- Bestimmte Online-Spiele
- Einzelne Netzwerk-LAN-Ports des Routers
- Spezifisches Gerät nach MAC-Adresse

Um die Priorität des Datenverkehrs anzugeben, müssen Sie eine Richtlinie für den Datenverkehrstyp erstellen und die Richtlinie der Tabelle mit den QoS-Richtlinien auf dem Bildschirm **QoS Setup** (QoS-Konfiguration) hinzufügen. Die Tabelle mit den QoS-Richtlinien enthält bereits viele gängige Anwendungen und Online-Spiele, deren Leistung durch die QoS-Einstellungen erhöht werden kann.

QoS für Anwendungen und Online-Spiele

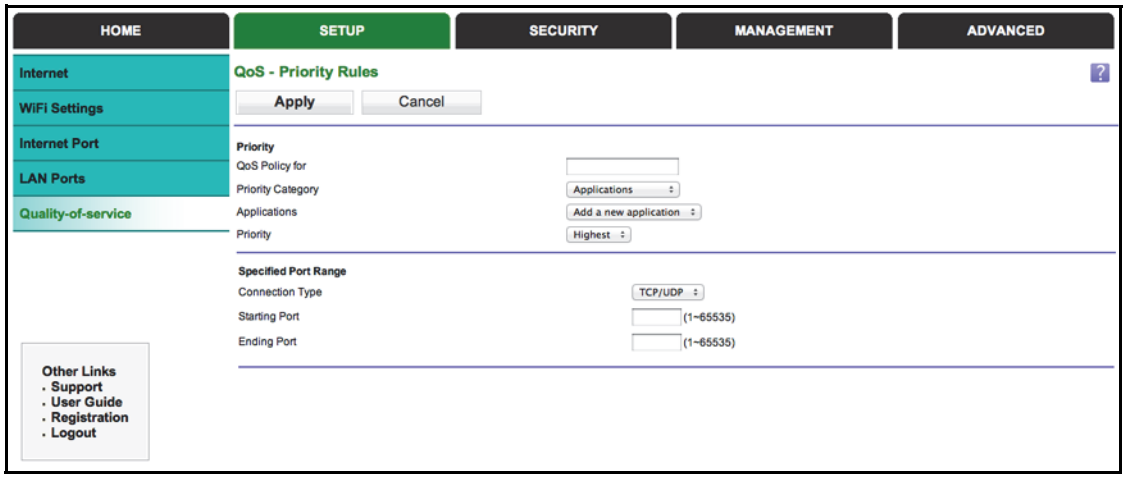
➢ **So erstellen Sie eine QoS-Richtlinie für Anwendungen und Online-Spiele:**

1. Aktivieren Sie auf dem Bildschirm **QoS Setup** (QoS-Konfiguration) das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
2. Klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen), um die vorhandenen Prioritätsregeln anzuzeigen.



Sie können eine Regel bearbeiten oder löschen, indem Sie die entsprechende Optionsschaltfläche aktivieren und auf die Schaltfläche **Edit** (Bearbeiten) oder **Delete** (Löschen) klicken. Außerdem können Sie alle Regeln löschen, indem Sie auf die Schaltfläche **Delete All** (Alle löschen) klicken.

3. Zum Hinzufügen einer Prioritätsregel blättern Sie bis zum Ende des Bildschirms **QoS Setup** (QoS-Konfiguration), und klicken Sie auf **Add Priority Rule** (Neue Prioritätsregel). Der folgende Bildschirm wird angezeigt:



4. Geben Sie in das Feld **QoS Policy for** (QoS-Richtlinie für) den Namen der Anwendung oder des Spiels ein.
5. Wählen Sie in der Liste **Priority Category** (Prioritätskategorie) entweder **Applications** (Anwendungen) oder **Online Gaming** (Online-Spiele) aus. In beiden Fällen wird eine Liste der Anwendungen oder Spiele aufgeführt.
6. Sie können einen vorhandenen Eintrag aus der Liste auswählen oder blättern und **Add a New Application** (Neue Anwendung hinzufügen) bzw. **Add a New Game** (Neues Spiel hinzufügen) auswählen.

   Wenn Sie einen Eintrag hinzufügen, wird der Bildschirm **Priority Rules** (Prioritätsregeln) erweitert.

   a. Geben Sie in das Feld **QoS Policy for** (QoS-Richtlinie für) einen Namen für die neue Anwendung oder das neue Spiel ein.

   b. Wählen Sie in der Liste **Connection Type** (Verbindungstyp) entweder **TCP** oder **UDP** oder beides (**TCP/UDP**) aus. Geben Sie die Portnummer oder den Portnummernbereich für die Anwendung oder das Spiel an.
7. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr beim Internetzugriff im Vergleich zu anderen Anwendungen und Datenverkehrstypen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
8. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS-Konfiguration) zurück.

QoS für einen Router-LAN-Port

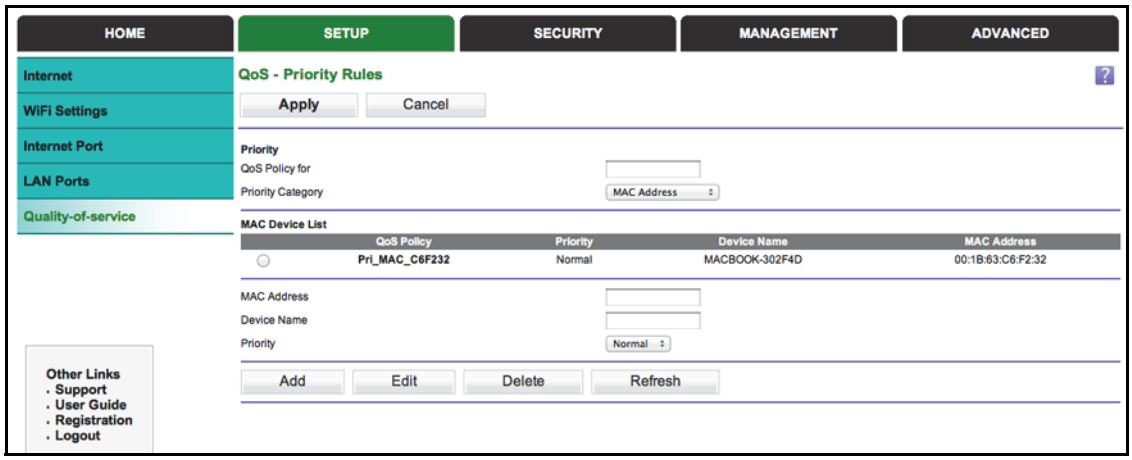
➢ **So erstellen Sie eine QoS-Richtlinie für ein Gerät, das an einen der LAN-Ports des Routers angeschlossen ist:**

1. Wählen Sie **Setup** (Konfiguration) > **Quality of Service** aus, um den Bildschirm **QoS Setup** (QoS-Konfiguration) anzuzeigen. Aktivieren Sie das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
2. Klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen).
3. Klicken Sie auf die Schaltfläche **Add Priority Rule** (Neue Prioritätsregel).
4. Wählen Sie aus der Liste **Priority Category** (Prioritätskategorie) die Option **Ethernet LAN Port** (Netzwerk-LAN-Port) aus.
5. Wählen Sie aus der Liste **LAN Port** (LAN-Port) den LAN-Port aus.
6. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr dieses Ports beim Internetzugriff im Vergleich zu anderen Anwendungen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
7. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS-Konfiguration) zurück.
8. Klicken Sie im Bildschirm **QoS Setup** (QoS-Konfiguration) auf **Apply** (Übernehmen).

QoS für eine MAC-Adresse

➢ **So erstellen Sie eine QoS-Richtlinie für Datenverkehr von einer bestimmten MAC-Adresse:**

1. Wählen Sie **Setup** (Konfiguration) > **Quality of Service** aus, und klicken Sie auf die Schaltfläche **Setup QoS Rule** (QoS-Regel festlegen). Der Bildschirm **QoS Setup** (QoS-Konfiguration) wird geöffnet.
2. Klicken Sie auf **Add Priority Rule** (Neue Prioritätsregel).
3. Wählen Sie aus der Liste **Priority Category** (Prioritätskategorie) die Option **MAC Address** (MAC-Adresse) aus:



4. Aktivieren Sie die Optionsschaltfläche des Geräts, falls es sich in der Liste der MAC-Geräte befindet. Der Richtlinienname, die MAC-Adresse und der Gerätename werden mit den Informationen aus der Liste der MAC-Geräte ausgefüllt. Klicken Sie auf **Refresh** (Aktualisieren), wenn sich das Gerät nicht in der Liste befindet. Falls es auch dann nicht angezeigt wird, müssen Sie diese Felder manuell ausfüllen.
5. Wählen Sie aus der Liste **Priority** (Priorität) die Priorität aus, die dem Datenverkehr dieses Geräts beim Internetzugriff im Vergleich zu anderen Anwendungen und Datenverkehrstypen zugeordnet werden soll. Die verfügbaren Optionen sind **Low** (Niedrig), **Normal**, **High** (Hoch) und **Highest** (Höchste).
6. Klicken Sie auf **Apply** (Übernehmen), um diese Regel in der Liste der QoS-Richtlinien zu speichern, und kehren Sie zum Bildschirm **QoS Setup** (QoS-Konfiguration) zurück.
7. Aktivieren Sie auf dem Bildschirm **QoS Setup** (QoS-Konfiguration) das Kontrollkästchen **Turn Internet Access QoS On** (QoS für Internetzugang aktivieren).
8. Klicken Sie auf **Apply** (Übernehmen).

Bearbeiten oder Löschen einer vorhandenen QoS-Richtlinie

➢ **So bearbeiten oder löschen Sie eine QoS-Richtlinie:**

1. Wählen Sie **Setup** (Konfiguration) > **Quality of Service** aus, um den Bildschirm **QoS Setup** (QoS-Konfiguration) anzuzeigen.
2. Aktivieren Sie die Optionsschaltfläche neben der QoS-Richtlinie, die Sie bearbeiten oder löschen möchten, und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Löschen** (Delete), um die QoS-Richtlinie zu entfernen.
   - Klicken Sie auf **Edit** (Bearbeiten), um die QoS-Richtlinie zu bearbeiten. Befolgen Sie die Anweisungen in den vorhergehenden Abschnitten, um die Richtlinieneinstellungen zu ändern.
3. Klicken Sie auf dem Bildschirm QoS Setup (QoS-Konfiguration) auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Sicherheitseinstellungen

4

Informationen auf der Registerkarte **Security** (Sicherheit)

Sie können viele Firewall-Einstellungen nach Ihren Erfordernissen anpassen. Dieses Kapitel enthält die folgenden Abschnitte:

- *Firewall-Regeln zur Steuerung des Netzwerkzugangs*
- *Konfigurieren der Seitensperrung*
- *Konfigurieren der Dienstsperre*
- *Einstellen der Zeitzone*
- *Zeitliches Planen von Diensten*
- *Konfigurieren von E-Mail-Warnmeldungen*
- *Konfigurieren der Portweiterleitung an lokale Server*
- *Konfigurieren des Port-Triggering*

Firewall-Regeln zur Steuerung des Netzwerkzugangs

Ihr Router verfügt über eine Firewall, die unbefugte Zugriffe auf Ihr WLAN-Netzwerk blockiert und autorisierte eingehende und ausgehende Kommunikation erlaubt. Autorisierte Kommunikation wird anhand von Regeln für eingehenden und ausgehenden Datenverkehr konfiguriert. Die Firewall bietet die folgenden zwei Standardregeln. Sie können benutzerdefinierte Regeln erstellen, um die ausgehende Kommunikation weiter einzuschränken oder die eingehende Kommunikation weiter zu öffnen:

- **Inbound** (Eingehend): Alle Zugriffe von außen sperren, außer Antworten auf Anfragen aus dem LAN.
- **Outbound** (Ausgehend): Alle Zugriffe aus dem LAN nach außen zulassen.

Eingangsregeln (Portweiterleitung)

Da der Router NAT (Network Address Translation) verwendet, wird Ihr Netzwerk vom Internet als eine einzige IP-Adresse erkannt. Benutzer von außerhalb können nicht direkt auf einen Ihrer lokalen Computer zugreifen. Durch die Definition einer Eingangsregel können Sie jedoch einen lokalen Server (z. B. einen Webserver oder Spieleserver) im Internet sichtbar und verfügbar machen.

Die Regel sorgt dafür, dass der Router eingehenden Datenverkehr für einen bestimmten Dienst auf Grundlage der Portnummer des Ziels an einen lokalen Server weiterleitet. Dieser Vorgang ist auch unter dem Namen Portweiterleitung bekannt. Das Zulassen eingehender Dienste führt zu Öffnungen in der Firewall. Aktivieren Sie nur die Ports, die für das Netzwerk erforderlich sind. Im Folgenden werden zwei Beispiele für Eingangsregeln erläutert.

Hinweis: Einige wohnsitzabhängige Breitband-ISP-Konten lassen die Ausführung von Serverprozessen (z. B. Web- oder FTP-Server) von Ihrem Standort nicht zu. Möglicherweise überprüft Ihr ISP regelmäßig, ob Server betrieben werden, und setzt Ihr Konto aus, wenn aktive Dienste an Ihrem Standort erkannt werden. Wenn Sie nicht sicher sind, lesen Sie die Richtlinien Ihres ISPs zur zulässigen Nutzung.

Ausgangsregeln (Dienstsperren)

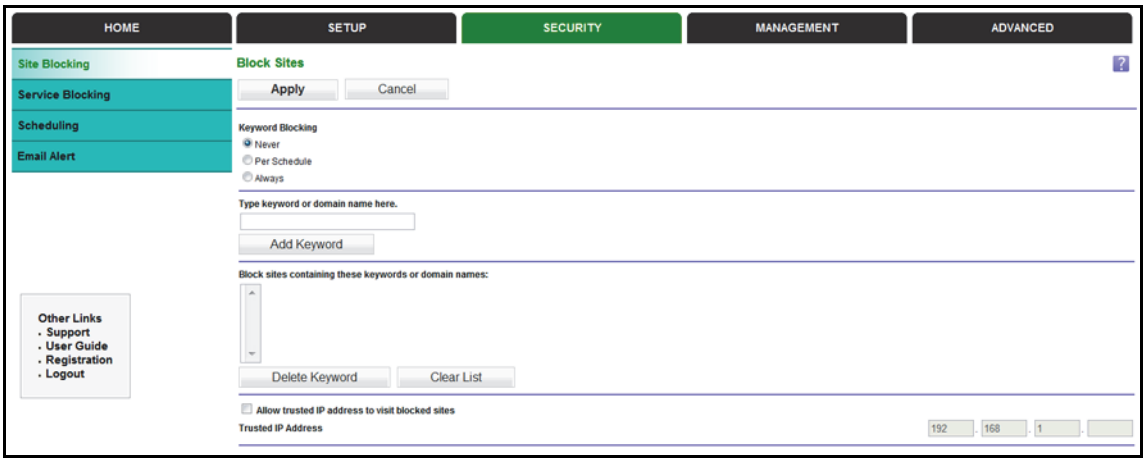
Sie können Computer in Ihrem lokalen Netzwerk blockieren, sodass bestimmte Internetdienste nicht verwendet werden können. Diese Funktion wird als Dienstsperre oder Portfilterung bezeichnet. Sie können eine Ausgangsregel hinzufügen, um Internetzugriff von einem lokalen Computer basierend auf dem Computer, der Internetwebsite, der Tageszeit und dem Diensttyp zu blockieren.

Konfigurieren der Seitensperrung

Mit der Stichwortsperre können Sie verhindern, dass bestimmte Arten von HTTP-Datenverkehr auf das Netzwerk zugreifen können. Die Sperre kann permanent oder nach einem Zeitplan eingerichtet werden.

➢ **So blockieren Sie den Datenverkehr:**

1. Wählen Sie **Security** (Sicherheit) > **Site Blocking** (Seitensperrung).



2. Wählen Sie eine der Optionen für die Stichwortsperre aus:
   - **Per Schedule** (Nach Zeitplan): Aktiviert die Stichwortsperre unter Berücksichtigung der Einstellungen auf dem Bildschirm **Schedule** (Zeitplan)
   - **Always** (Immer): Aktiviert die permanente Stichwortsperre unabhängig von den Einstellungen auf dem Bildschirm **Schedule** (Zeitplan)
3. Geben Sie ein Stichwort oder eine Domain in das Stichwortfeld ein, klicken Sie auf **Add Keyword** (Stichwort hinzufügen), und klicken Sie auf **Apply** (Übernehmen).

   Es werden bis zu 32 Einträge in der Stichwortliste unterstützt. Hier finden Sie einige Beispiele:

   - Geben Sie **XXX** an, um **http://www.badstuff.com/xxx.html** zu sperren.
   - Geben Sie **.com** an, um nur Internetseiten mit anderen Domainerweiterungen, wie **.edu** oder **.gov**, zuzulassen.
   - Geben Sie einen Punkt (**.**) ein, um den gesamten Zugriff auf das Internet zu sperren.

Löschen eines Stichworts oder einer Domain

➢ **So löschen Sie Stichwörter:**

1. Wählen Sie das Stichwort oder die Domain, das/die Sie von der Liste entfernen wollen.
2. Klicken Sie auf **Delete Keyword** (Stichwort löschen) und danach auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Angeben eines vertrauenswürdigen Computers

Sie können einen vertrauenswürdigen Computer von der Sperre und Protokollierung ausnehmen. Der ausgenommene Computer muss über eine statische IP-Adresse verfügen.

➢ **So geben Sie einen vertrauenswürdigen Computer an:**

1. Geben Sie die IP-Adresse in das Feld **Trusted IP Address** (Vertrauenswürdige IP-Adresse) ein.
2. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

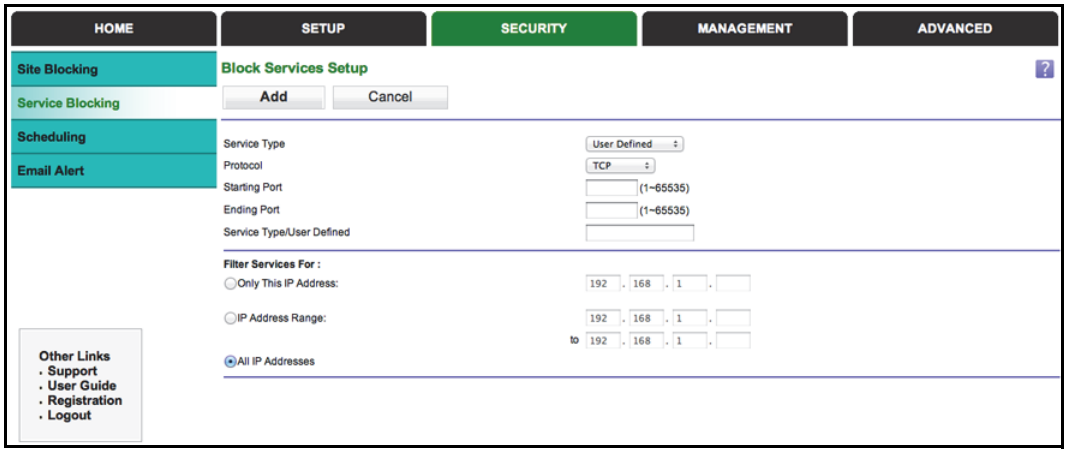
Konfigurieren der Dienstsperre

Dienste sind Funktionen, die auf Anfrage von Clientcomputern durch Servercomputer ausgeführt werden. Webserver liefern z. B. Webseiten, Zeitserver liefern Informationen zu Datum und Uhrzeit und Spiele-Hosts liefern Daten über die Züge anderer Spieler. Wenn ein Computer im Internet eine Dienstanfrage an einen Server-Computer richtet, ist der entsprechende Dienst durch eine Portnummer gekennzeichnet. Diese Nummer wird als Zielportnummer in den übertragenen IP-Paketen angegeben. Ein Paket, das mit der Zielportnummer 80 gesendet wird, ist beispielsweise eine HTTP-Anfrage (an den Webserver).

Die Dienstnummern für viele gebräuchliche Protokolle werden von der Internet Engineering Task Force (IETF unter *http://www.ietf.org/*) definiert und in RFC1700, „Assigned Numbers“ (Zugewiesene Nummern), veröffentlicht. Dienstnummern für andere Anwendungen werden gewöhnlich von den Herausgebern der Anwendung im Bereich 1024 bis 65535 gewählt. Auf dem Router ist bereits eine Liste mit vielen Dienstportnummern gespeichert, Sie können jedoch auch andere Portnummern auswählen.

➢ **So erstellen Sie eigene Dienstdefinitionen:**

1. Wählen Sie **Security** (Sicherheit) > **Service Blocking** (Dienstsperrung). Der folgende Bildschirm wird angezeigt:



2. Um einen Dienst zu erstellen, klicken Sie auf die Schaltfläche **Add** (Hinzufügen). Wenn Sie einen Dienst ändern möchten, wählen Sie ihn aus, und klicken Sie auf **Edit** (Bearbeiten).

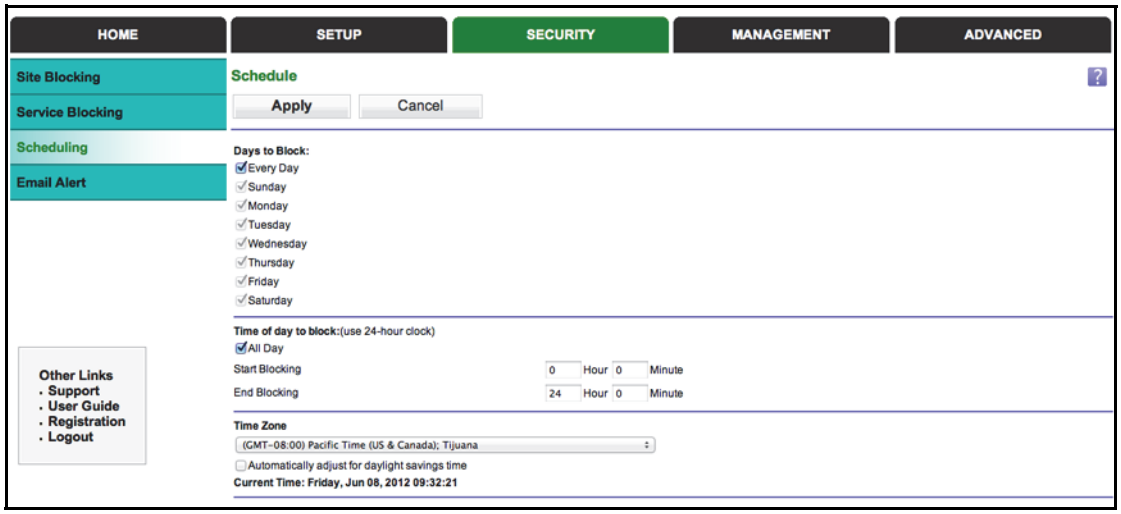
3. Geben Sie die folgenden Informationen an, um einen Dienst zu definieren oder zu bearbeiten.
   - **Name**: Geben Sie einen aussagekräftigen Namen für den Dienst ein.
   - **Type** (Typ): Wählen Sie den richtigen Typ für den Dienst aus. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP**. Die Optionen sind TCP, UDP und TCP/UDP.
   - **Start Port** (Erster Port) und **Finish Port** (Letzter Port): Wenn ein Portbereich erforderlich ist, geben Sie den Bereich hier ein. Wenn nur ein Port erforderlich ist, geben Sie in beide Felder denselben Wert ein.
4. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Einstellen der Zeitzone

Der Router nutzt das NTP-Protokoll (Network Time Protocol) zum Abruf der aktuellen Uhrzeit und des Datums von einem der NTP-Server im Internet.

➢ **So stellen Sie die Zeitzone ein:**

1. Wählen Sie **Security** (Sicherheit) > **Schedule** (Zeitplan).



2. Wählen Sie Ihre Zeitzone aus. Diese Einstellung legt den Zeitplans für Sperren und die zeitliche Bestimmung von Protokolleinträgen fest.
3. Falls sich Ihre Zeitzone in der Sommerzeit befindet, aktivieren Sie das Kontrollkästchen **Adjust for daylight savings time** (An Sommer-/Winterzeit anpassen) um der Standardzeit eine Stunde hinzuzufügen.

   Hinweis: *Falls in Ihrer Region zwischen Sommer- und Winterzeit unterschieden wird, aktivieren Sie **Adjust for daylight savings time** (An Sommer-/Winterzeit anpassen) am ersten Tag, und deaktivieren Sie es nach dem letzten Tag.*

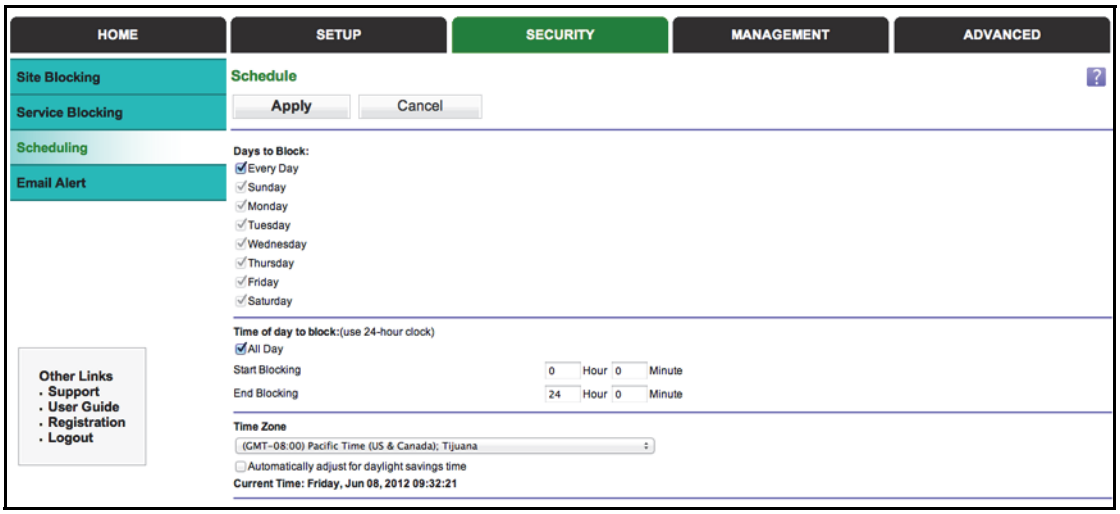
4. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Zeitliches Planen von Diensten

Wenn Sie Dienstsperren im Bildschirm **Block Services** (Dienste sperren) bzw. Port-Forwarding im Bildschirm **Ports** aktiviert haben, können Sie in einem Zeitplan festlegen, wann die Sperrung erfolgen soll bzw. wann der Zugriff nicht eingeschränkt wird.

➢ **So richten Sie einen Zeitplan für Dienste ein:**

1. Wählen Sie **Security** (Sicherheit) > **Schedule** (Zeitplan).



2. Zur Sperrung von Internetdiensten anhand eines Zeitplans wählen Sie **Every Day** (Alle) oder einen oder mehrere Tage.
3. Wenn die Zugriffsbeschränkungen an den gewählten Wochentagen rund um die Uhr gelten sollen, wählen Sie **All Day** (Ganztätig). Andernfalls geben Sie die Zeitpunkte in die Felder **Start Blocking** (Sperre aktivieren um) und **End Blocking** (Sperre deaktivieren um) ein.

   Hinweis: *Geben Sie die Werte im 24-Stunden-Format ein. Beispiel: 10:30 bedeutet 10 Uhr und 30 Minuten morgens, und 22:30 bedeutet 10 Uhr und 30 Minuten abends. Wenn Sie die Startzeit nach der Endzeit ansetzen, gilt der Zeitplan über den Tageswechsel hinaus.*

4. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Konfigurieren von E-Mail-Warnmeldungen

Wenn Sie Protokolle und Warnungen per E-Mail erhalten möchten, geben Sie Ihre E-Mail-Informationen auf dem Bildschirm **E-mail** (E-Mail) ein, und geben Sie an, welche Warnungen Sie mit welcher Regelmäßigkeit erhalten möchten.

Wählen Sie **Security** (Sicherheit) > **E-Mail Alert** (E-Mail-Warnmeldung) aus, um den folgenden Bildschirm anzuzeigen:

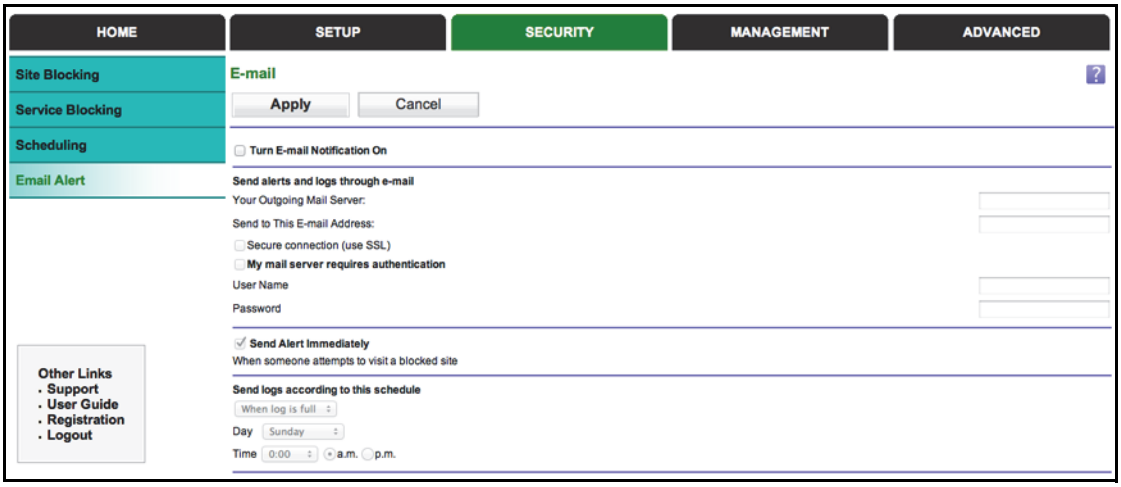


Abbildung 6. Bildschirm E-Mail

- **Turn E-mail Notification On** (E-Mail-Benachrichtigung aktivieren): Aktivieren Sie dieses Kontrollkästchen, wenn Sie vom Router Protokolle und Benachrichtigungen per E-Mail erhalten möchten.
- **Send to This E-mail Address** (Mailadresse des Empfängers): Geben Sie die E-Mail-Adresse ein, an die Protokolle und Benachrichtigungen gesendet werden sollen. Diese E-Mail-Adresse wird auch als Absender angegeben. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Warnmeldungen per E-Mail gesendet.
- **Your Outgoing Mail Server** (Server für den E-Mail-Versand): Geben Sie den Namen oder die IP-Adresse des SMTP-Servers Ihres ISP (für abgehende E-Mail-Nachrichten) ein (z. B. mail.meinISP.de). Möglicherweise finden Sie diese Informationen in den Konfigurationseinstellungen Ihres E-Mail-Programms. Geben Sie die E-Mail-Adresse ein, an die Protokolle und Benachrichtigungen gesendet werden sollen. Diese E-Mail-Adresse wird auch als Absender angegeben. Wenn Sie dieses Feld leer lassen, werden keine Protokolle und Warnmeldungen per E-Mail gesendet.
- **My mail server requires authentication** (Mailserver erfordert Authentifizierung): Wenn Sie einen Postausgangsserver verwenden, der von Ihrem gegenwärtigen ISP bereitgestellt wird, müssen Sie dieses Feld nicht aktivieren. Wenn Sie ein E-Mail-Konto verwenden, das nicht von Ihrem ISP bereitgestellt wird, aktivieren Sie dieses Feld, und geben Sie die erforderlichen Zugangsdaten (Benutzername und Passwort) an.
- **Send Alerts Immediately** (Benachrichtigungen sofort senden): Aktivieren Sie das entsprechende Kontrollkästchen, wenn Sie sofortige Benachrichtigungen über wichtige sicherheitsrelevante Ereignisse wünschen, beispielsweise einen erkannten Angriff, einen Port-Scan oder den versuchten Zugriff auf eine gesperrte Seite.

- **Send logs according to this schedule** (Protokolle nach diesem Zeitplan senden): Damit geben Sie an, wie oft die Protokolle gesendet werden sollen: Keine, Stündlich, Täglich, Wöchentlich oder Bei vollem Protokoll.
  - **Days** (Tage): Gibt an, an welchem Wochentag das Protokoll gesendet werden soll. Dies ist relevant, wenn das Protokoll wöchentlich gesendet wird.
  - **Time** (Uhrzeit): Gibt die Tageszeit an, zu der das Protokoll gesendet werden soll. Dies ist relevant, wenn das Protokoll täglich oder wöchentlich gesendet wird.

Hinweis: Wenn die Option für wöchentliche, tägliche oder stündliche Benachrichtigung gewählt wurde und das Protokoll vor Ablauf der angegebenen Zeit voll ist, wird es automatisch an die angegebene E-Mail-Adresse gesendet. Nach dem Senden des Protokolls wird dieses automatisch aus dem Speicher des Routers gelöscht. Wenn der Router die Protokolldatei nicht per E-Mail senden kann, wird der Protokoll-Zwischenspeicher möglicherweise zu voll. In diesem Fall überschreibt der Router das Protokoll und löscht seinen Inhalt.

Portweiterleitung und Port-Triggering

Standardmäßig blockiert der Router eingehenden Datenverkehr aus dem Internet auf Ihre Computer, mit Ausnahme von Antworten auf abgehenden Datenverkehr. Möglicherweise müssen Sie Ausnahmen für diese Regel festlegen, z. B. in den folgenden Fällen:

- Remote-Computer im Internet müssen auf einen Server im lokalen Netzwerk zugreifen.
- Bestimmte Anwendungen und Spiele können andernfalls nicht ordnungsgemäß ausgeführt werden, da ihre Antworten vom Router nicht immer erkannt werden.

Der Router bietet zwei Funktionen für die Erstellung dieser Ausnahmen: Portweiterleitung und Port-Triggering. Die folgenden Abschnitte enthalten Hintergrundinformationen zu diesem Thema, um die Funktion von Portweiterleitung und Port-Triggering zu erläutern und die Unterschiede zwischen diesen beiden Konzepten aufzuzeigen.

Grundlegende Informationen zum Remote-Computerzugriff

Wenn ein Computer im Netzwerk auf einen Computer im Internet zugreifen muss, sendet der Computer Ihrem Router eine Meldung mit der Quell- und Zieladresse und den Prozessinformationen. Vor der Weiterleitung der Meldung an den Remote-Computer muss der Router die Quellinformationen ändern und die Sitzung für den Datenaustausch erstellen und nachverfolgen, damit Antworten zurück auf den Computer geleitet werden können.

Es folgt ein Beispiel für normalen abgehenden Datenverkehr und die darauf folgenden eingehenden Antworten:

1. Sie öffnen einen Browser, und Ihr Betriebssystem weist dieser Browsersitzung die Portnummer 5678 zu.
2. Sie geben in das URL-Feld die Adresse http://www.beispiel.de ein, und Ihr Computer erstellt eine Meldung für die Anforderung einer Webseite mit den folgenden Adress- und Portinformationen. Die Anforderung wird an den Router gesendet.

   Quelladresse: Die IP-Adresse des Computers

   Quellportnummer: 5678, die Portnummer der Browsersitzung

   Zieladresse: Die IP-Adresse der URL **www.beispiel.de**, die Ihr Computer durch eine Anfrage beim DNS-Server ermittelt

   Zielportnummer: 80, die Standardportnummer eines Webserver-Prozesses
3. Der Router erstellt einen Eintrag in der Tabelle für interne Sitzungen und beschreibt diese Sitzung für den Datenaustausch zwischen Ihrem Computer und dem Webserver unter www.beispiel.de. Bevor die Anforderung der Webseite an www.beispiel.de gesendet wird, speichert der Router die ursprünglichen Informationen und ändert dann die Quellinformationen der Anforderung, d. h., er führt eine Network Address Translation (NAT) durch:
   - Die Quelladresse wird durch die öffentliche IP-Adresse des Routers ersetzt. Dies ist notwendig, da Ihr Computer eine private IP-Adresse verwendet, die nicht weltweit eindeutig ist und im Internet nicht verwendet werden kann.
   - Die Quellportnummer wird zu einer vom Router zugewiesenen Nummer geändert, z. B. 33333. Dies ist notwendig, da zwei Computer unabhängig voneinander dieselbe Sitzungsnummer verwenden könnten.

   Der Router sendet daraufhin die Anforderung über das Internet an den Webserver unter **www.beispiel.de**.
4. Der Webserver unter **www.beispiel.de** verfasst eine Rücknachricht mit den angeforderten Webseitendaten. Die Rücknachricht enthält die folgenden Adress- und Portinformationen. Der Webserver sendet diese Antwort danach an den Router.

   Quelladresse: Die IP-Adresse der URL www.beispiel.de

   Quellportnummer: 80, die Standardportnummer eines Webserver-Prozesses

   Zieladresse: Die öffentliche IP-Adresse des Routers

   Zielportnummer: 33333
5. Nach dem Empfang der eingehenden Nachricht überprüft der Router über die Sitzungstabelle, ob es eine aktive Sitzung für die Portnummer 33333 gibt. Falls der Router eine aktive Sitzung findet, ändert er die Nachricht, um die ursprünglichen Adressinformationen wiederherzustellen, die durch den NAT-Vorgang ersetzt wurden. Der Router sendet die Antwort an den Computer, der die Webseite **www.beispiel.de** anzeigt. Die Nachricht enthält jetzt die folgenden Adress- und Portinformationen.

   Quelladresse: Die IP-Adresse der URL www.beispiel.de

Quellportnummer: 80, die Standardportnummer eines Webserver-Prozesses

Zieladresse: Die IP-Adresse des Computers

Zielportnummer: 5678, die Browsersitzung, von der die erste Anforderung gesendet wurde

6. Nach Beendigung der Browsersitzung entdeckt der Router möglicherweise einen Zeitraum der Inaktivität in der Kommunikation. Der Router entfernt daraufhin die Sitzungsinformationen aus der Sitzungstabelle, und eingehender Datenverkehr wird für die Portnummer 33333 nicht mehr akzeptiert.

Port-Triggering zum Öffnen eingehender Ports

Im vorhergehenden Beispiel werden Anforderungen von Ihrem Router über eine bestimmte Dienstportnummer an einen Remote-Computer gesendet. Die Antworten des Remote-Computers an Ihren Router werden an diese Portnummer geleitet. Wenn der Remote-Server eine Antwort zurück an eine andere Portnummer sendet, akzeptiert der Router sie nicht und verwirft sie. Einige Anwendungsserver jedoch (z. B. FTP- und IRC-Server) senden Antworten zurück an mehrere Portnummern. Mit der Funktion **Port-Triggering** des Routers können Sie den Router so einrichten, dass er zusätzliche eingehende Ports öffnet, wenn ein bestimmter Ausgangs-Port eine Sitzung initiiert.

Ein Beispiel dafür ist IRC (Internet Relay Chat). Ihr Computer stellt eine Verbindung mit einem IRC-Server am Zielport 6667 her. Der IRC-Server antwortet nicht nur über den ursprünglichen Quellport, sondern sendet außerdem eine Identifizierungsnachricht über Port 113 an den Computer. Mit Port-Triggering können Sie dem Router Folgendes mitteilen: „Wenn eine Sitzung über den Zielport 6667 initiiert wird, muss auch eingehender Datenverkehr über Port 113 den Ursprungscomputer erreichen.“ Mit ähnlichen Schritten wie im vorhergehenden Beispiel sind im Folgenden die Ergebnisse der definierten Port-Triggering-Regel dargestellt:

1. Sie öffnen ein IRC-Clientprogramm, um eine Chatsitzung auf dem Computer zu starten.
2. Der IRC-Client verfasst eine Anforderungsnachricht an einen IRC-Server über die Zielportnummer 6667, die Standardportnummer für einen IRC-Servervorgang. Der Computer sendet diese Antwort danach an den Router.
3. Der Router erstellt einen Eintrag in der Tabelle für interne Sitzungen und beschreibt diese Sitzung für den Datenaustausch zwischen Ihrem Computer und dem IRC-Server. Der Router speichert die ursprünglichen Informationen, führt eine Network Address Translation (NAT) für die Quelladresse und den Quellport aus und sendet diese Anforderung über das Internet an den IRC-Server.
4. Unter Beachtung der Port-Triggering-Regel und mit Berücksichtigung der Zielportnummer 6667 erstellt der Router einen zusätzlichen Sitzungseintrag, um den für Port 113 eingehenden Datenverkehr an den Computer zu senden.
5. Der IRC-Server sendet eine Rücknachricht über den durch NAT zugewiesenen Quellport (z. B. 33333, wie im vorherigen Beispiel) als Zielport an den Router. Darüber hinaus sendet der IRC-Server eine Identifizierungsnachricht mit Zielport 113 an den Router.

6. Nach dem Empfang der eingehenden Nachricht an den Zielport 33333 überprüft der Router über die Sitzungstabelle, ob es eine aktive Sitzung für die Portnummer 33333 gibt. Nachdem er die aktive Sitzung gefunden hat, stellt der Router die zuvor über NAT ersetzten ursprünglichen Adressinformationen wieder her und sendet die Rückantwort an den Computer.
7. Nach dem Empfang der eingehenden Nachricht an den Zielport 113 überprüft der Router die Sitzungstabelle und findet dort eine aktive Sitzung für die Portnummer 113, die Ihrem Computer zugeordnet ist. Der Router ersetzt die IP-Zieladresse der Nachricht durch die IP-Adresse des Computers und leitet die Nachricht an den Computer weiter.
8. Nach Beendigung der Chatsitzung entdeckt der Router möglicherweise einen Zeitraum der Inaktivität in der Kommunikation. Der Router entfernt daraufhin die Sitzungsinformationen aus der Sitzungstabelle, und eingehender Datenverkehr wird für die Portnummern 33333 oder 113 nicht mehr akzeptiert.

Damit Sie Port-Triggering konfigurieren können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt. Außerdem müssen Sie die Nummer des Ausgangs-Ports kennen, der die Öffnung der Eingangs-Ports auslöst. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

Hinweis: Die Triggering-Anwendung kann immer nur auf einem Computer verwendet werden.

Portweiterleitung zur Zulassung externer Hostkommunikation

In den beiden vorhergehenden Beispielen wurde eine Anwendungssitzung mit einem Server-Computer im Internet von Ihrem Computer initiiert. Möglicherweise müssen Sie jedoch zulassen, dass ein Client-Computer im Internet eine Verbindung zu einem Server-Computer in Ihrem Netzwerk herstellt. Normalerweise ignoriert der Router eingehenden Datenverkehr, der nicht als Antwort auf Ihren ausgehenden Datenverkehr gesendet wird. Mit der Portweiterleitung können Sie Ausnahmen für diese Standardregel konfigurieren.

Eine häufige Anwendung der Portweiterleitung kann durch die Umkehrung der Client-Server-Beziehung aus dem vorherigen Webserver-Beispiel demonstriert werden. In diesem Fall muss der Browser eines Remote-Computers auf einen Webserver zugreifen, der auf einem Computer im lokalen Netzwerk ausgeführt wird. Mit der Portweiterleitung können Sie dem Router Router Folgendes mitteilen: „Wenn eingehender Datenverkehr über Port 80 (Standardportnummer für einen Webserver-Prozess) empfangen wird, muss dieser an den lokalen Computer unter 192.168.1.123 weitergeleitet werden.“ Im Folgenden sind die Ergebnisse der definierten Portweiterleitungsregel dargestellt:

1. Ein Benutzer eines Remote-Computers öffnet einen Browser und fordert eine Webseite von **www.beispiel.de** an, die zur öffentlichen IP-Adresse Ihres Routers aufgelöst wird. Der Remote-Computer erstellt eine Anforderung für eine Webseite mit den folgenden Zielinformationen:

   Zieladresse: Die IP-Adresse von www.beispiel.de, die mit der Adresse des Routers übereinstimmt

Zielportnummer: 80, die Standardportnummer eines Webserver-Prozesses

Der Remote-Computer sendet danach diese Anforderung über das Internet an den Router.

2. Der Router empfängt die Anforderung und überprüft, ob es in der Regeltabelle eine Regel gibt, die die Art des eingehenden Datenverkehrs an Port 80 abdeckt. In der Portweiterleitungsregel wird angegeben, dass der eingehende Datenverkehr an Port 80 an die lokale IP-Adresse 192.168.1.123 weitergeleitet werden soll. Deshalb ändert der Router die Zielinformationen in der Anforderung:

   Die Zieladresse wird durch 192.168.1.123 ersetzt.

   Der Router sendet die Anforderung danach an das lokale Netzwerk.

3. Ihr Webserver unter 192.168.1.123 empfängt die Anforderung und verfasst eine Rücknachricht mit den angeforderten Webseitendaten. Der Webserver sendet diese Antwort danach an den Router.
4. Der Router führt eine Network Address Translation (NAT) für die Quell-IP-Adresse aus und sendet diese Anforderung über das Internet an den Remote-Computer, der die Webseite von www.beispiel.de anzeigt.

Damit Sie die Portweiterleitung konfigurieren können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung oder die entsprechenden Benutzergruppen und Newsgruppen wenden.

Unterschiede zwischen Portweiterleitung und Port-Triggering

In den folgenden Punkten werden die Unterschiede zwischen Portweiterleitung und Port-Triggering zusammengefasst:

- Port-Triggering kann von jedem beliebigen Computer im Netzwerk verwendet werden, jedoch immer nur von jeweils einem Computer.
- Die Portweiterleitung wird für einen einzelnen Computer im Netzwerk konfiguriert.
- Beim Port-Triggering müssen Sie die IP-Adresse des Computers im Voraus kennen. Die IP-Adresse wird automatisch erfasst.
- Für die Portweiterleitung müssen Sie die IP-Adresse des Computers während der Konfiguration angeben, und die IP-Adresse darf sich nicht ändern.
- Für das Port-Triggering müssen durch bestimmten abgehenden Datenverkehr Eingangs-Ports geöffnet werden. Die Triggering-Ports werden nach einem bestimmten Zeitraum der Inaktivität geschlossen.
- Die Portweiterleitung ist immer aktiv und muss nicht durch Triggering ausgelöst werden.

Konfigurieren der Portweiterleitung an lokale Server

Mit der Portweiterleitung können Sie zulassen, dass bestimmte eingehende Datenverkehrstypen Server im lokalen Netzwerk erreichen. Beispiel: Sie möchten einen lokalen Webserver, FTP-Server oder Spieleserver über das Internet sichtbar und verfügbar machen.

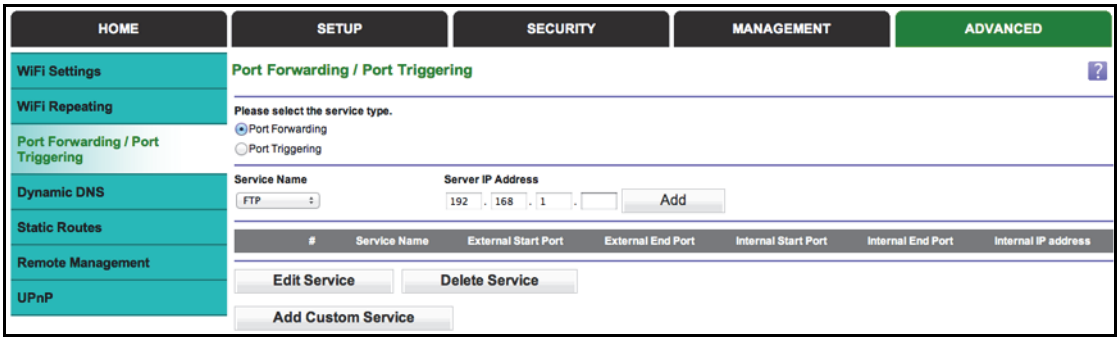
Mit dem Bildschirm **Port Forwarding** (Portweiterleitung) können Sie den Router so konfigurieren, dass bestimmte eingehende Protokolle an Computer in Ihrem lokalen Netzwerk weitergeleitet werden. Neben Servern für bestimmte Anwendungen können Sie auch einen DMZ-Standardserver festlegen, an den alle anderen eingehenden Protokolle weitergeleitet werden.

Ermitteln Sie zunächst, welche Art von Dienst, Anwendung oder Spiel Sie bereitstellen möchten. Machen Sie die lokale IP-Adresse des Computers ausfindig, der den Dienst bereitstellen soll. Der Server-Computer muss stets dieselbe IP-Adresse haben.

➢ **So konfigurieren Sie die Portweiterleitung:**

Tipp: Legen Sie über die Adressreservierungsfunktion des N150R-Routers fest, dass dem Server-Computer immer dieselbe IP-Adresse zugewiesen wird.

1. Wählen Sie **Advanced Setup** (Erweiterte Einrichtung) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus. Der folgende Bildschirm wird angezeigt:



Als Diensttyp wird die Portweiterleitung ausgewählt.

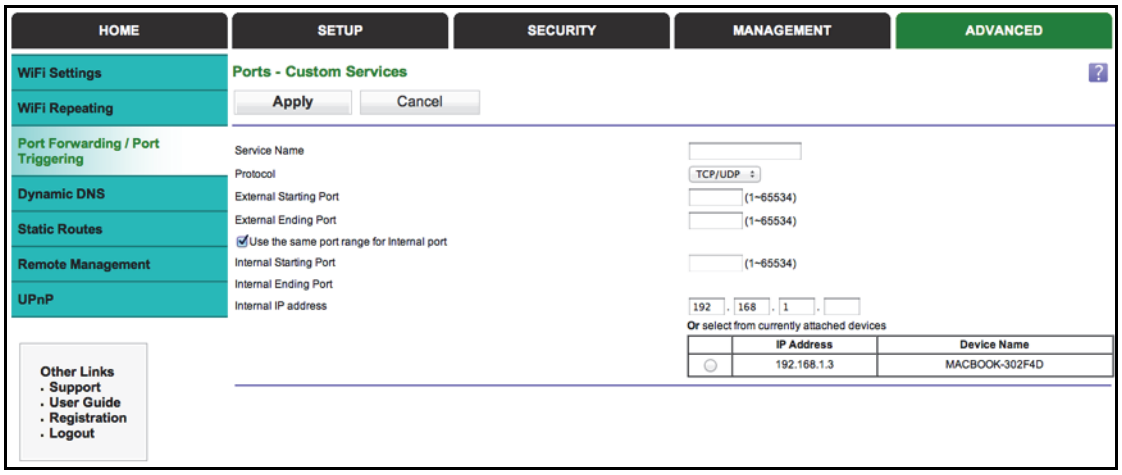
2. Wählen Sie aus der Dropdown-Liste **Service Name** (Dienstname) den Dienst bzw. das Spiel aus, der bzw. das in Ihrem Netzwerk gehostet werden soll. Sollte der Dienst nicht in der Liste angezeigt werden, lesen Sie die Informationen unter *Hinzufügen eines benutzerdefinierten Diensts* auf Seite 52.
3. Geben Sie in das entsprechende Feld für die Server-IP-Adresse die letzte Ziffer der IP-Adresse Ihres lokalen Computers ein, über den der Dienst bereitgestellt wird.
4. Klicken Sie auf **Add** (Hinzufügen). Der Dienst wird in der Liste auf dem Bildschirm angezeigt.

Hinzufügen eines benutzerdefinierten Diensts

Zum Definieren von Diensten, Spielen oder Anwendungen, die nicht in der Liste **Service Name** (Dienstname) angezeigt werden, benötigen Sie zuerst die Portnummern oder Portnummernbereiche der Anwendung. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

➢ **So fügen Sie einen benutzerdefinierten Dienst hinzu:**

1. Wählen Sie **Advanced** (Erweitert) > **Advanced Setup** (Erweiterte Einrichtung) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus.
2. Wählen Sie **Port Forwarding** (Portweiterleitung) als Diensttyp aus.
3. Klicken Sie auf die Schaltfläche **Add Custom Service** (Benutzerdefinierten Dienst hinzufügen), um den folgenden Bildschirm anzuzeigen:



4. Geben Sie einen aussagefähigen Namen in das Feld **Service Name** (Dienstname) ein.
5. Wählen Sie in der Liste Protocol (Protokoll) das Protokoll aus. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP** aus.
6. Geben Sie in das Feld **Starting Port** (Erster Port) die erste Portnummer ein.
   - Wenn die Anwendung nur einen Port verwendet, geben Sie dieselbe Portnummer in das Feld Ending Port (Letzter Port) ein.
   - Wenn die Anwendung einen Bereich aus mehreren Ports verwendet, geben Sie die Nummer des letzten Ports in diesem Bereich in das Feld **Ending Port** (Letzter Port) ein.
7. Geben Sie in das Feld für die Server-IP-Adresse die IP-Adresse Ihres lokalen Computers ein, über den der Dienst bereitgestellt wird.
8. Klicken Sie auf **Apply** (Übernehmen). Der Dienst wird in der Liste auf dem Bildschirm **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) angezeigt.

Bearbeiten oder Löschen eines Portweiterleitungseintrags

➢ **So bearbeiten oder löschen Sie einen Portweiterleitungseintrag:**

1. Aktivieren Sie in der Tabelle die Optionsschaltfläche neben dem Dienstnamen.
2. Klicken Sie auf **Edit Service** (Dienst bearbeiten) oder **Delete Service** (Dienst löschen).

Anwendungsbeispiel: Veröffentlichen eines lokalen Webservers

Wenn Sie einen Webserver in Ihrem lokalen Netzwerk hosten, können Sie über die Portweiterleitung festlegen, dass Webanforderungen von anderen Personen im Internet Ihren Webserver erreichen.

➢ **So veröffentlichen Sie einen lokalen Webserver:**

1. Weisen Sie dem Webserver entweder eine feste IP-Adresse oder eine dynamische IP-Adresse mit DHCP-Adressreservierung zu. In diesem Beispiel vergibt der Router stets die IP-Adresse 192.168.1.33 an den Webserver.
2. Konfigurieren Sie den Router im Bildschirm Port Forwarding (Portweiterleitung) so, dass der HTTP-Dienst an die lokale Adresse Ihres Webservers unter **192.168.1.33** weitergeleitet wird. HTTP (Port 80) ist das Standardprotokoll für Webserver.
3. (Optional) Registrieren Sie einen Hostnamen bei einem dynamischen DNS-Dienst, und konfigurieren Sie den Router für die Verwendung des Namens, wie unter *Dynamisches DNS* auf Seite 75 beschrieben. Damit ein Remote-Benutzer über das Internet auf Ihren Webserver zugreifen kann, muss er die IP-Adresse kennen, die Ihnen von Ihrem ISP zugewiesen wurde. Falls Sie einen dynamischen DNS-Dienst verwenden, kann der Remote-Benutzer Ihren Server jedoch über einen benutzerfreundlichen Internetnamen erreichen, z. B. **meinnetzwerk.dyndns.org**.

Konfigurieren des Port-Triggering

Port-Triggering ist eine dynamische Erweiterung der Portweiterleitung, die in den folgenden Fällen hilfreich sein kann:

- Mehr als ein lokaler Computer benötigt die Port-Weiterleitung für dieselbe Anwendung (jedoch nicht gleichzeitig).
- Eine Anwendung muss Eingangs-Ports öffnen, die sich vom Ausgangs-Port unterscheiden.

Bei Aktivierung des Port-Triggering überwacht der Router abgehenden Datenverkehr und sucht nach einem angegebenen abgehenden Trigger-Port. Wenn der Router abgehenden Datenverkehr an diesem Port registriert, speichert er die IP-Adresse des lokalen Computers, der die Daten gesendet hat. Der Router öffnet daraufhin vorübergehend den angegebenen Eingangs-Port bzw. die Eingangs-Ports und leitet eingehenden Datenverkehr für die Triggering-Ports an den Triggering-Computer weiter.

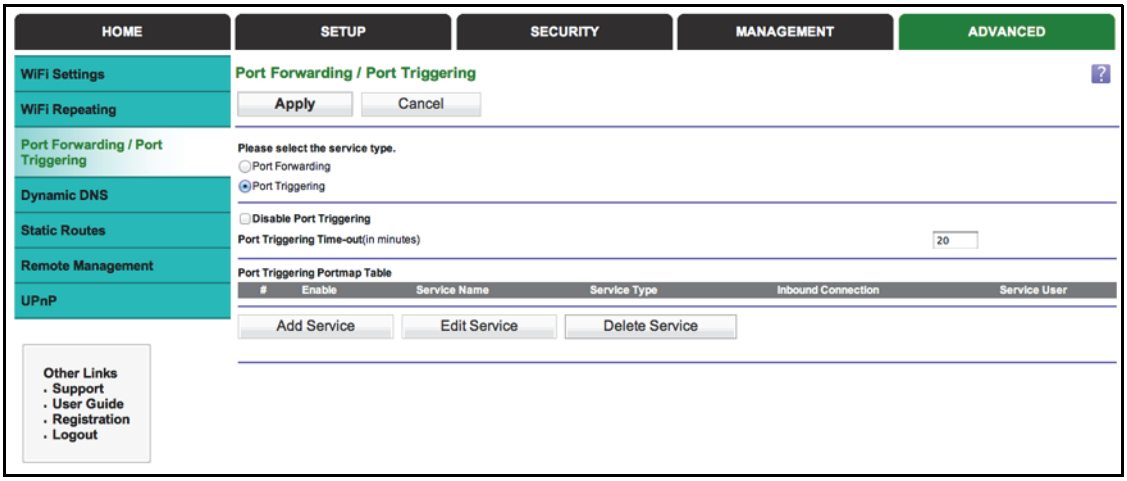
Bei der Portweiterleitung wird eine statische Zuordnung einer Portnummer oder eines Portbereichs für einen einzelnen lokalen Computer erstellt. Beim Port-Triggering können Ports für einen beliebigen Computer, der diese erfordert, geöffnet und wieder geschlossen werden, nachdem der Zugang nicht mehr benötigt wird.

Hinweis: Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie auch UPnP (Universal Plug and Play) aktivieren. Befolgen Sie dazu die Anweisungen unter *Universal Plug and Play* auf Seite 79.

Damit Sie Port-Triggering einrichten können, müssen Sie wissen, welche Eingangs-Ports die Anwendung benötigt, und Sie müssen die Nummer des Ausgangs-Ports kennen, der die Öffnung der Eingangs-Ports auslöst. Diese Informationen erhalten Sie normalerweise, indem Sie sich an den Herausgeber der Anwendung, Benutzergruppen oder Newsgruppen wenden.

➢ **So konfigurieren Sie Port-Triggering:**

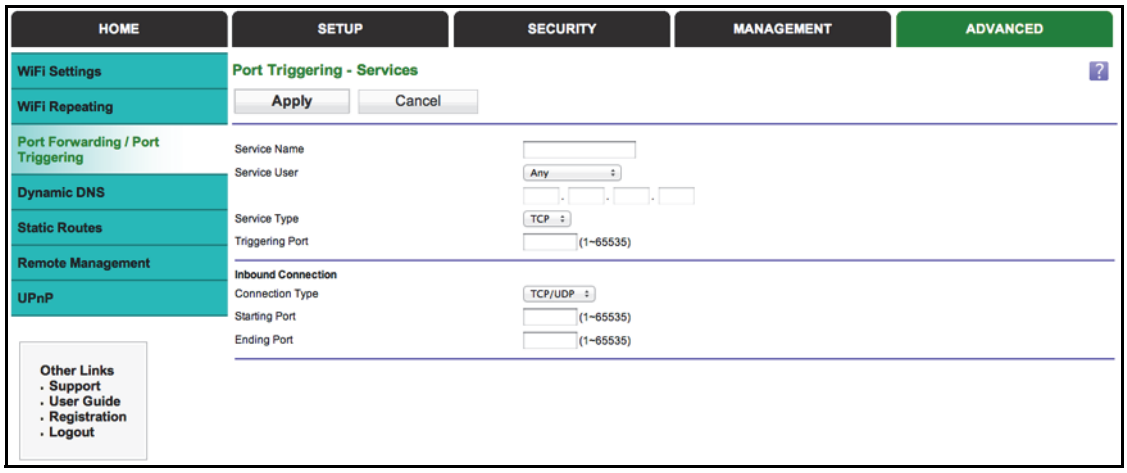
1. Wählen Sie **Advanced** (Erweitert) > **Port Forwarding/Port Triggering** (Portweiterleitung/Port-Triggering) aus.
2. Aktivieren Sie die Optionsschaltfläche **Port Triggering** (Port-Triggering), um die Informationen zum Port-Triggering anzuzeigen.



3. Deaktivieren Sie das Kontrollkästchen **Disable Port Triggering** (Port-Triggering deaktivieren), falls es aktiviert ist.

Hinweis: *Wenn Sie nach der Konfiguration des Port-Triggering das Kontrollkästchen **Disable Port Triggering** (Port-Triggering deaktivieren) aktivieren, wird diese Funktion deaktiviert. Die Port-Triggering-Konfigurationsdaten, die Sie dem Router hinzugefügt haben, bleiben jedoch erhalten, auch wenn sie nicht verwendet werden.*

4. Geben Sie im Feld **Port Triggering Timeout** (Leerlaufzeit für Port-Triggering) einen Wert von bis zu 9999 Minuten ein.
5. Dieser Wert bestimmt, wie lange ein Eingangs-Port geöffnet bleibt, wenn keine weiteren Daten über diesen Port übertragen werden. Die Eingangs-Ports werden geschlossen, wenn der Zeitraum der Inaktivität verstrichen ist. Dies ist erforderlich, da der Router sonst nicht erkennen kann, wann die Anwendung beendet wurde.
6. Klicken Sie auf **Add Service** (Dienst hinzufügen), um den folgenden Bildschirm anzuzeigen:



7. Geben Sie einen aussagefähigen Dienstnamen in das Feld **Service Name** (Dienstname) ein.
8. Wählen Sie in der Liste **Service User** (Dienstbenutzer) die Standardoption **Any** (Alle) aus, um zuzulassen, dass dieser Dienst von allen Computern im Internet verwendet werden kann. Wählen Sie ansonsten **Single Address** (Einzelne Adresse), und geben Sie die IP-Adresse eines einzelnen Computers ein, wenn nur dieser eine Computer den Dienst nutzen soll.
9. Wählen Sie als Diensttyp **TCP**, **UDP** oder beides (**TCP/UDP**) aus. Wenn Sie nicht sicher sind, wählen Sie **TCP/UDP**.
10. Geben Sie in das Feld **Triggering Port** (Triggering-Port) die Nummer des Ports für den abgehenden Datenverkehr ein, der dafür sorgt, dass die Eingangs-Ports geöffnet werden.
11. Füllen Sie die Portinformationen für die Eingangsverbindung in den Feldern **Connection Type** (Verbindungstyp), **Starting Port** (Erster Port) und **Ending Port** (Letzter Port) aus.
12. Klicken Sie auf **Apply** (Übernehmen). Der Dienst wird in der Zuordnungstabelle für Port-Triggering angezeigt.

Netzwerkverwaltung

5

Optionen auf der Registerkarte **Management** (Verwaltung)

Dieses Kapitel enthält die folgenden Abschnitte:

- *Aktualisieren der Router-Firmware*
- *Manuelle Suche nach Firmware-Aktualisierungen*
- *Sichern der Einstellungen*
- *Ändern des Passworts*
- *Anzeigen des Routerstatus*
- *Anzeigen von angeschlossenen Geräten*
- *Protokolle*

Aktualisieren der Router-Firmware

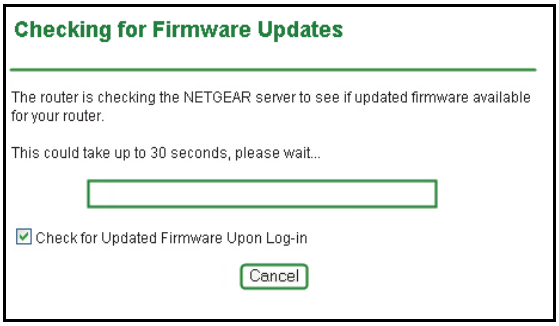
Die Router-Firmware (Routing-Software) ist auf einem Flash-Speicher gespeichert. Bei der Anmeldung an Ihrem Router prüft er standardmäßig die On Networks-Webseite auf neue Firmware und benachrichtigt Sie, falls es eine neuere Version gibt.

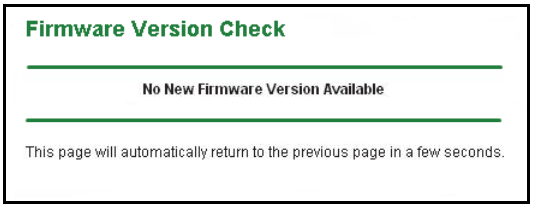
WARNUNG:

Achten Sie beim Hochladen der Firmware auf den Router darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

Automatische Firmwareprüfung

Wenn die automatische Firmwareprüfung aktiviert ist, führt der Router die Prüfung durch und benachrichtigt Sie darüber, ob eine Aktualisierung verfügbar ist oder nicht.


Checking for Firmware Updates
The router is checking the NETGEAR server to see if updated firmware available for your router.
This could take up to 30 seconds, please wait...
Check for Updated Firmware Upon Log-in
Cancel


Firmware Version Check
No New Firmware Version Available
This page will automatically return to the previous page in a few seconds.

➢ **So prüfen Sie die Firmware automatisch:**

1. Klicken Sie auf **Yes** (Ja), um den Router zu gestatten, die neue Firmware herunterzuladen und zu installieren Der Aktualisierungsvorgang kann einige Minuten in Anspruch nehmen. Nach dem Hochladen der Firmware wird der Router neu gestartet.
2. Rufen Sie die N150R-Supportseite auf, und lesen Sie die Informationen zur neuen Version der Firmware, um herauszufinden, ob Sie den Router nach der Aktualisierung neu konfigurieren müssen.

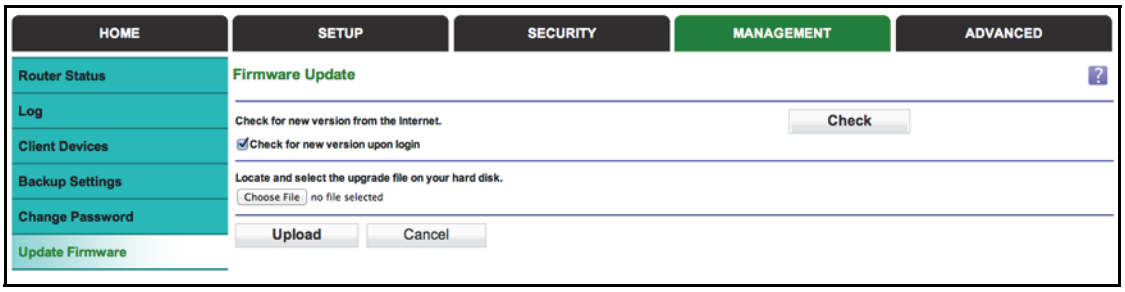
Hinweis: Wenn Sie die Meldung **Firmware needs to be reloaded** (Firmware muss neu geladen werden) erhalten, bedeutet dies, dass ein Problem mit der Firmware des Routers festgestellt wurde. Befolgen Sie die Bildschirmanweisungen, um das Problem zu beheben.

Beenden der automatischen Firmwareprüfung

Sie können die automatische Firmwareprüfung nach Belieben abschalten und manuell nach aktualisierten Versionen suchen. Siehe *Manuelle Suche nach Firmware-Aktualisierungen* auf Seite 58. So schalten Sie die automatische Firmwareprüfung bei der Anmeldung aus:

➢ **So beenden Sie die automatische Firmwareprüfung:**

1. Wählen Sie **Management** (Verwaltung) > **Update Firmware** (Firmware aktualisieren).
2. Deaktivieren Sie das Kontrollkästchen **Check for new version upon login** (Beim Anmelden nach neuer Version suchen).



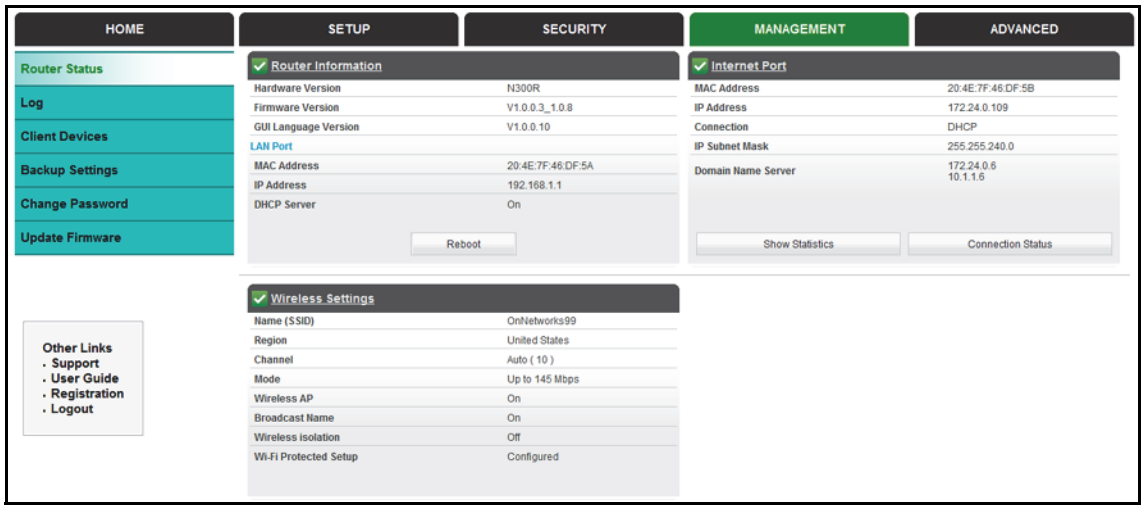
Manuelle Suche nach Firmware-Aktualisierungen

Sie können über den Bildschirm **Router Upgrade** (Router aktualisieren) die On Networks-Webseite nach neueren Versionen der Firmware für Ihr Produkt durchsuchen.

WARNUNG:

Achten Sie beim Hochladen der Firmware auf den Router darauf, dass der Vorgang *nicht* unterbrochen wird (z. B. durch Schließen des Browserfensters, Klicken auf einen Link oder Laden einer neuen Seite). Wenn eine Unterbrechung im Browser stattfindet, wird die Firmware möglicherweise fehlerhaft installiert.

1. Melden Sie sich am Router an, wählen Sie **Manage** (Verwalten) > **Router Status** (Routerstatus), und notieren Sie die Firmwareversion des Routers.



2. Rufen Sie die N150R-Supportseite auf der On Networks-Website unter *http://www.on-networks.com/support* auf.
3. Vergleichen Sie die Nummer der aktuell verfügbaren Firmware mit der Firmwareversion Ihres Routers. Wenn die Version auf der On Networks-Website neuer ist, laden Sie die Datei von der N150R-Supportseite auf Ihren Computer herunter.
4. Melden Sie sich am Router an, und wählen Sie **Management** (Verwaltung) > **Update Firmware** (Firmware aktualisieren).
5. Klicken Sie auf **Browse** (Durchsuchen), und navigieren Sie zum Firmware-Image, das Sie auf den Computer heruntergeladen haben (die Datei hat die Endung .img oder .chk).
6. Klicken Sie auf **Upload** (Hochladen), um die Firmware auf den Router zu übertragen.

   Nach dem Hochladen der Firmware wird der Router neu gestartet. Der Aktualisierungsvorgang dauert in der Regel ungefähr eine Minute. Lesen Sie die Versionshinweise der neuen Firmware, um zu überprüfen, ob Sie den Router nach der Aktualisierung neu konfigurieren müssen.

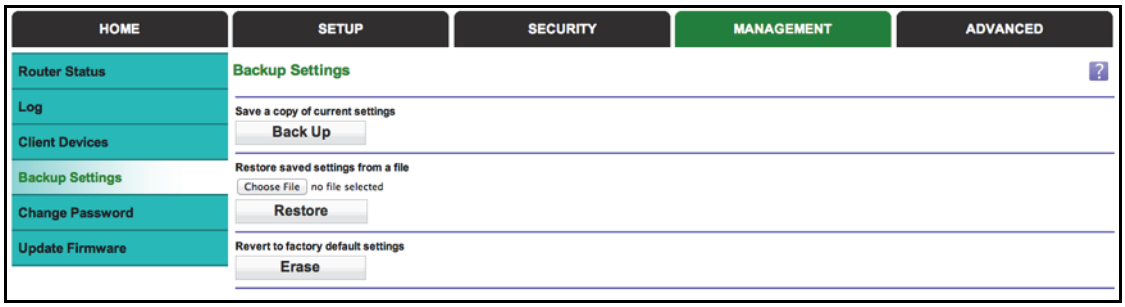
Sichern der Einstellungen

Die Konfigurationseinstellungen des Routers werden in einer Konfigurationsdatei gespeichert (*.cfg). Diese Datei kann auf Ihrem Computer gesichert, wiederhergestellt oder auch zum Zurücksetzen auf die werkseitigen Voreinstellungen verwendet werden.

Sichern

➢ **So sichern Sie die Konfigurationsdatei des Routers:**

1. Wählen Sie **Management** (Verwaltung)> **Backup Settings** (Einstellungen sichern). Der folgende Bildschirm wird angezeigt:



2. Klicken Sie auf **Save** (Speichern), um eine Kopie der aktuellen Einstellungen zu speichern.
3. Wählen Sie einen Speicherort für die Datei mit der Erweiterung **.cfg** auf einem Computer im Netzwerk.

Wiederherstellen

➢ **So stellen Sie die Konfigurationsdatei wieder her:**

1. Geben Sie den vollständigen Netzwerkpfad zur Datei ein, oder klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um die Datei zu suchen.
2. Wenn Sie die Datei mit der Erweiterung **.cfg** gefunden haben, klicken Sie auf die Schaltfläche **Restore** (Wiederherstellen), um die Datei auf den Router hochzuladen.

   Nach diesem Vorgang wird der Router neu gestartet.

Löschen

Klicken Sie auf die Schaltfläche **Erase** (Löschen), um den Router auf die werkseitigen Voreinstellungen zurückzusetzen. Durch Löschen wird das Passwort in **password** und die LAN-IP-Adresse in **192.168.1.1** geändert und das DHCP des Routers aktiviert.

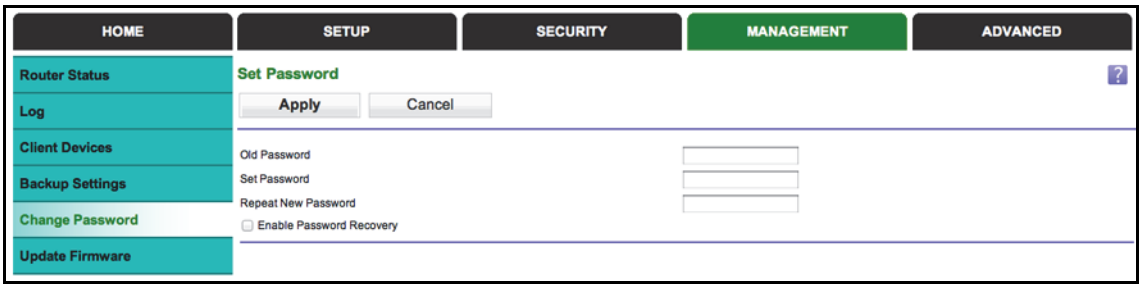
Ändern des Passworts

Aus Sicherheitsgründen hat der Router eigene Zugangsdaten (Benutzername und Passwort). Standardmäßig lauten diese **admin** und **password**. Sie können und sollten diese Zugangsdaten ändern und sichere Daten wählen, die Sie sich leicht merken können. Das ideale Passwort enthält keine Wörter aus Wörterbüchern jeglicher Sprache und besteht aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Es kann aus bis zu 30 Zeichen bestehen.

Hinweis: Der Benutzername und das Passwort des Routers unterscheiden sich vom Benutzernamen und Passwort für die Anmeldung zum Herstellen einer Internetverbindung. Weitere Informationen zu Anmeldearten finden Sie in *Anmeldearten* auf Seite 14.

➢ **So ändern Sie das Passwort und die Anmeldezeitbeschränkung:**

1. Wählen Sie **Management** (Verwaltung) > **Change Password** (Passwort ändern). Der folgende Bildschirm wird angezeigt:



2. Geben Sie das alte Passwort ein.
3. Geben Sie das neue Passwort zweimal ein.
4. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Nach Änderung des Passworts müssen Sie sich erneut anmelden, um die Konfiguration fortzuführen. Hinweis: Wenn Sie die Geräteeinstellungen für den Router gesichert haben, sollten Sie diesen Vorgang nun erneut durchführen, damit das geänderte Passwort in die Sicherungsdatei aufgenommen wird. Informationen zur Sicherung Ihrer Netzwerkkonfiguration finden Sie unter *Sichern* auf Seite 60.

Passwortwiederherstellung

On Networks empfiehlt, die Passwortwiederherstellung zu aktivieren, wenn Sie das Passwort für den Admin-Benutzer des Routers ändern. Wenn Sie das Passwort vergessen, können Sie es wiederherstellen. Die Wiederherstellung wird in Internet Explorer, Firefox und Chrome unterstützt, jedoch nicht in Safari.

➢ **So richten Sie die Passwortwiederherstellung ein:**

1. Aktivieren Sie das Kontrollkästchen **Enable Password Recovery** (Passwortwiederherstellung aktivieren).
2. Wählen Sie zwei Sicherheitsfragen aus, und beantworten Sie sie.
3. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

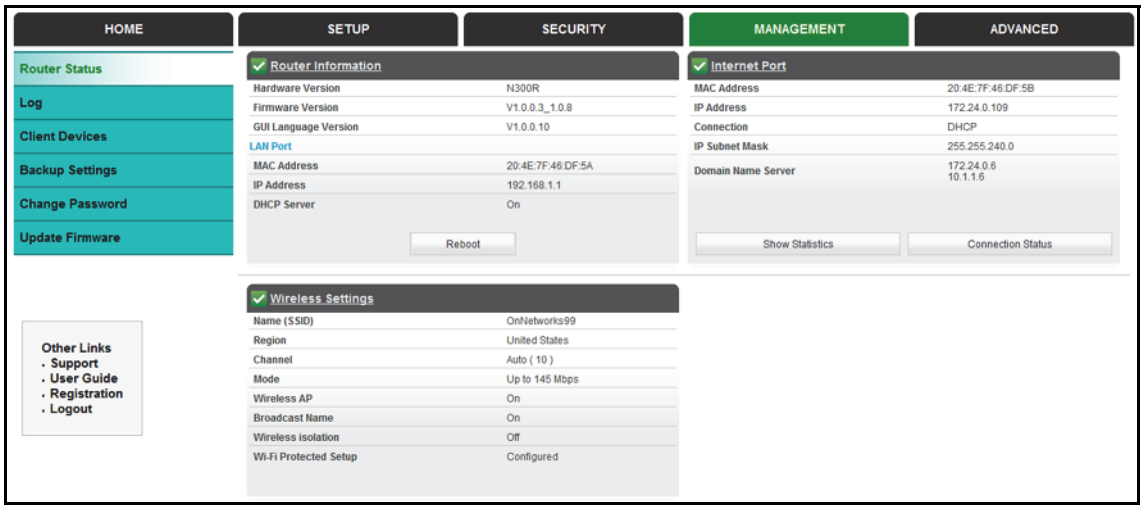
Wenn Sie über den Browser auf den Router zugreifen, wird das Anmeldefenster geöffnet. Bei Aktivierung der Passwortwiederherstellung wird die Passwortwiederherstellung gestartet, nachdem Sie auf **Cancel** (Abbrechen) geklickt haben. Sie können daraufhin die gespeicherten Antworten auf die Sicherheitsfragen eingeben, um das Passwort wiederherzustellen.

Anzeigen des Routerstatus

Der Bildschirm **Router Status** (Routerstatus) zeigt Status- und Auslastungsinformationen an.

➢ **So zeigen Sie den Routerstatus an:**

Wählen Sie **Management** (Verwaltung) > **Router Status** (Routerstatus). Der folgende Bildschirm wird angezeigt.



Folgende Informationen werden angezeigt:

Hardware and Firmware Version (Hardware- und Firmwareversion): Das Hardwaremodell und die aktuell aktive Firmwareversion.

GUI Language Version (Sprachversion der Benutzeroberfläche): Die aktuell gewählte Sprache.

Internet-Porteinstellungen

MAC Address (MAC-Adresse): Die MAC-Adresse des DSL-Ports.

IP Address (IP-Adresse): Die IP-Adresse des Internetports. Wenn keine IP-Adresse angezeigt wird, konnte der Router keine Verbindung zum Internet herstellen.

Connection (Verbindung): Der Wert hängt von Ihrem ISP ab.

IP Subnet Mask (IP-Subnetzmaske): Die IP-Subnetzmaske des Internetports.

Gateway IP Address (Gateway-IP-Adresse): Bei Computern, die für die Nutzung von DHCP konfiguriert sind, wird diese IP-Adresse als Gateway zum Internet verwendet.

Domain Name Server (DNS-Server): Die DNS-Server-IP-Adresse des Routers. Diese Adressen werden normalerweise automatisch vom ISP bezogen.

LAN-Port (Lokale Ports)

MAC Address (MAC-Adresse): Die LAN-Port-MAC-Adresse des Routers.

IP Address (IP-Adresse): Die Router LAN-Port-IP-Adresse. Die Standardeinstellung ist 192.168.1.1.

DHCP: Ist DHCP ausgeschaltet, so weist der Router PCs im LAN keine IP-Adressen zu. Ist DHCP eingeschaltet, so weist der Router PCs im LAN IP-Adressen zu.

IP Subnet Mask (IP-Subnetzmaske): Die vom Router-LAN verwendete IP-Subnetzmaske. Die Standardeinstellung ist 255.255.255.0.

Modem

ADSL Firmware Version (Version der ADSL-Firmware): Die Version der Firmware.

Modem Status (Modemstatus): Der Verbindungsstatus des Modems.

DownStream Connection Speed (Downstream-Verbindungsgeschwindigkeit): Das Modem erhält in dieser Geschwindigkeit Daten über die DSL-Leitung.

UpStream Connection Speed (Upstream-Verbindungsgeschwindigkeit): Das Modem übermittelt in dieser Geschwindigkeit Daten über die DSL-Leitung.

VPI: Die Einstellung zum Virtual Path Identifier.

VCI: Die Einstellung zum Virtual Channel Identifier.

Access Point

Unter *WiFi-Setup* auf Seite 24 finden Sie eine ausführliche Beschreibung dieser Einstellungen.

Name (SSID) (Netzwerkname [SSID]): Der Name des WLAN-Netzwerks (Service-Set ID).

Region: Das Land, in dem das Gerät für den Gebrauch eingerichtet ist.

Channel (Kanal): Der aktuelle Kanal, der die Betriebsfrequenz bestimmt.

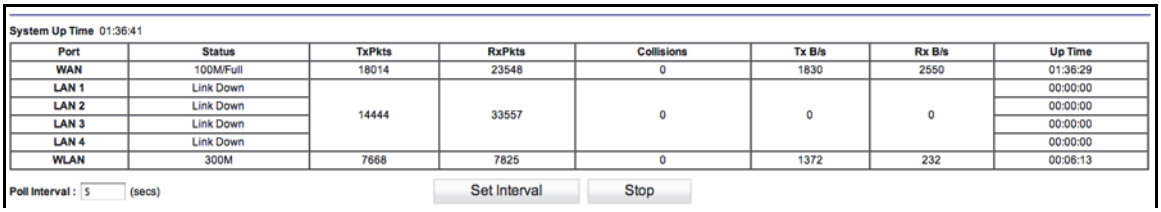
Mode (Modus): Die aktuelle maximale Datenübertragungsrate in MBit/s.

Wireless AP (WLAN-AP): Zeigt an, ob die Access Point-Funktion aktiviert ist. Wenn diese Funktion nicht aktiviert ist, leuchtet die WLAN-LED vorn am Router nicht.

Broadcast Name (Broadcast für Netzwerknamen): Zeigt an, ob der Router so konfiguriert ist, dass er seine SSID sendet.

Anzeigen der Statistik

Klicken Sie auf die Schaltfläche **Show Statistics** (Statistik anzeigen) im Bildschirm **Router Status** (Routerstatus). Ein ähnlicher Bildschirm wie der Folgende wird angezeigt:



System Up Time 01:36:41

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	18014	23548	0	1830	2550	01:36:29
LAN 1	Link Down	14444	33557	0	0	0	00:00:00
LAN 2	Link Down						00:00:00
LAN 3	Link Down						00:00:00
LAN 4	Link Down						00:00:00
WLAN	300M	7668	7825	0	1372	232	00:06:13

Poll Interval : 5 (secs) Set Interval Stop

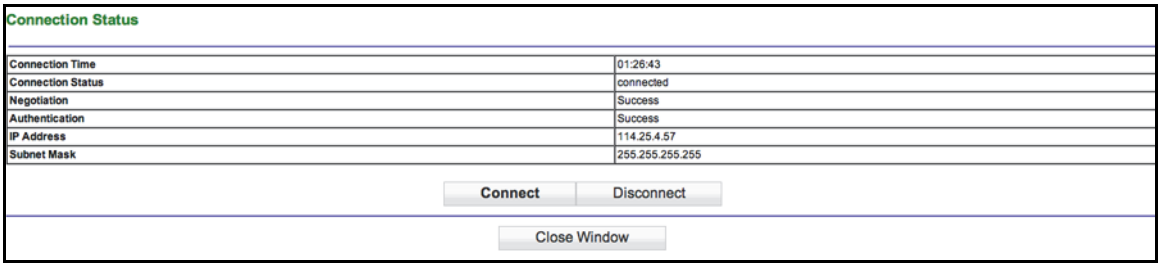
Port

Die Statistiken für die WAN- (Internet), LAN- (lokalen) und WLAN-Ports. Für jeden Port zeigt der Bildschirm Folgendes an:

- **Status**: Der Verbindungsstatus
- **TxPkts** (Übertragene Pakete): Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen übertragen wurden.
- **RxPkts** (Empfangene Pakete): Die Anzahl der Pakete, die seit dem letzten Zurücksetzen oder manuellen Löschen empfangen wurden.
- **Collisions** (Kollisionen): Die Anzahl der Kollisionen seit dem letzten Zurücksetzen oder manuellen Löschen.
- **Tx B/s** (Übertragene Bytes pro Sekunde): Die aktuelle Auslastung der Leitung (in Prozent der momentan genutzten Bandbreite).
- **Rx B/s** (Empfangene Bytes pro Sekunde): Die durchschnittliche Auslastung.
- **Up Time** (Laufzeit): Die verstrichene Zeit seit dem letzten Neustart oder Zurücksetzen.

Verbindungsstatus

Klicken Sie im Bildschirm **Router Status** (Routerstatus) auf die Schaltfläche **Connection Status** (Verbindungsstatus):



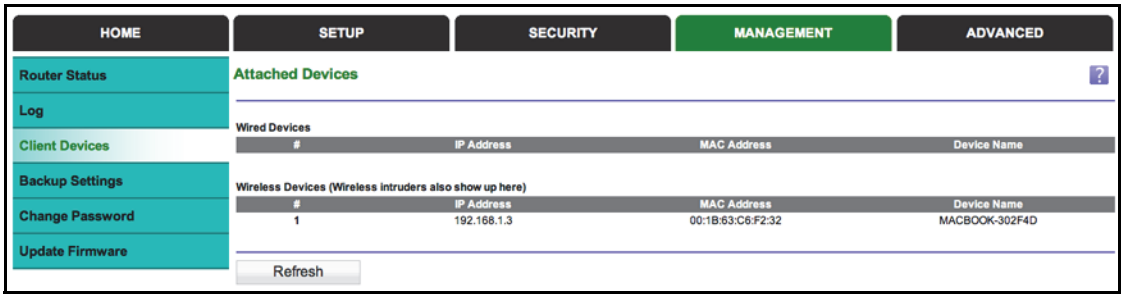
- **Connection Time** (Verbindungsdauer): Die verstrichene Zeit seit der letzten Verbindung mit dem Internet über den Internetport.
- **Connection Status** (Verbindungsstatus): Der Status der Verbindung.
- **Negotiation** (Abstimmung): An oder Aus.
- **Authentication** (Authentifizierung): An oder Aus.
- **Getting IP Address** (IP-Adresse beziehen): Die dem WAN-Port durch den ISP zugewiesene IP-Adresse.
- **Subnet Mask** (Subnetzmaske): Die dem WAN-Port durch den ISP zugewiesene Netzwerkmaske.

Anzeigen von angeschlossenen Geräten

Auf dem Bildschirm Attached Devices (Angeschlossene Geräte) werden alle IP-Geräte angezeigt, die der Router im lokalen Netzwerk erkannt hat.

➢ **So zeigen Sie die angeschlossenen Geräte an:**

Wählen Sie **Management** (Verwaltung) > **Client Devices** (Client-Geräte).



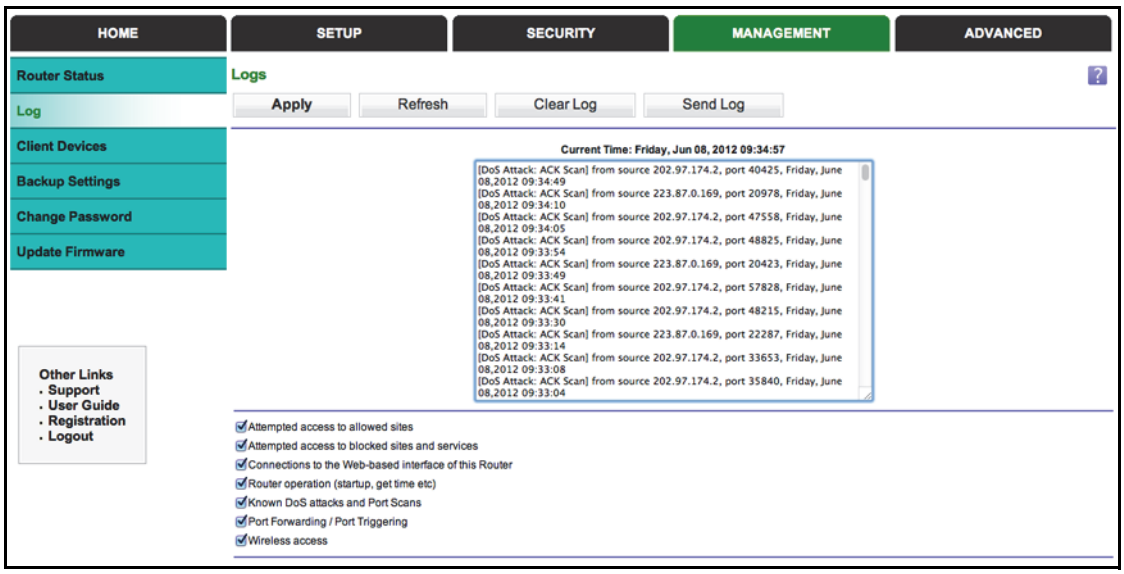
Für jedes Gerät zeigt die Tabelle die IP-Adresse, den Gerätenamen (sofern verfügbar) und die MAC-Adresse. Bei einem Neustart des Routers gehen die Tabellendaten verloren, bis der Router die Geräte wieder erkennt. Um den Router zur Suche nach angeschlossenen Geräten zu zwingen, klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren).

Protokolle

Der Router protokolliert sicherheitsrelevante Ereignisse wie abgelehnte eingehende Dienstanforderungen, Erkundungsgänge durch Hacker oder auch Anmeldungen durch den Administrator. Wenn Sie auf dem Bildschirm "Internetseiten sperren" einen Contentfilter aktivieren, werden auf dem Bildschirm "Protokolle" Zugriffsversuche auf gesperrte Seiten durch Benutzer im Netzwerk angezeigt. Wenn Sie die E-Mail-Benachrichtigung aktivieren, werden diese Protokolle per E-Mail versendet.

➢ **So zeigen Sie das Protokoll an:**

Wählen Sie **Management** (Verwaltung) > **Logs** (Protokolle). Daraufhin erscheint ein Bildschirm wie der folgende:


HOME
SETUP
SECURITY
MANAGEMENT
ADVANCED
Router Status
Log
Client Devices
Backup Settings
Change Password
Update Firmware
Logs
Apply
Refresh
Clear Log
Send Log
Current Time: Friday, Jun 08, 2012 09:34:57
[DoS Attack: ACK Scan] from source 202.97.174.2, port 40425, Friday, June 08,2012 09:34:49
[DoS Attack: ACK Scan] from source 223.87.0.169, port 20978, Friday, June 08,2012 09:34:10
[DoS Attack: ACK Scan] from source 202.97.174.2, port 47558, Friday, June 08,2012 09:34:05
[DoS Attack: ACK Scan] from source 202.97.174.2, port 48825, Friday, June 08,2012 09:33:54
[DoS Attack: ACK Scan] from source 223.87.0.169, port 20423, Friday, June 08,2012 09:33:49
[DoS Attack: ACK Scan] from source 202.97.174.2, port 57828, Friday, June 08,2012 09:33:41
[DoS Attack: ACK Scan] from source 202.97.174.2, port 48215, Friday, June 08,2012 09:33:30
[DoS Attack: ACK Scan] from source 223.87.0.169, port 22287, Friday, June 08,2012 09:33:14
[DoS Attack: ACK Scan] from source 202.97.174.2, port 33653, Friday, June 08,2012 09:33:08
[DoS Attack: ACK Scan] from source 202.97.174.2, port 35840, Friday, June 08,2012 09:33:04
Other Links
. Support
. User Guide
. Registration
. Logout
Attempted access to allowed sites
Attempted access to blocked sites and services
Connections to the Web-based interface of this Router
Router operation (startup, get time etc)
Known DoS attacks and Port Scans
Port Forwarding / Port Triggering
Wireless access

Mithilfe der Kontrollkästchen **Include in Log** (In Protokoll aufnehmen) können Sie auswählen, welche Ereignisse protokolliert werden sollen. Sie können die Protokolle auf einen Computer schreiben, auf dem ein Syslog-Programm läuft. Zur Aktivierung dieser Funktion wählen Sie **Broadcast on LAN** (Per LAN übertragen) oder geben die IP-Adresse des Servers ein, auf den die Syslog-Datei geschrieben wird. Die Sicherheitsprotokolleinträge enthalten die folgenden Informationen:

- **Datum und Uhrzeit**: Datum und Uhrzeit der Aufzeichnung des Protokolleintrags.
- **Beschreibung oder Vorgehensweise**. Die Art des Ereignisses und auf welche Weise vorgegangen wurde, falls zutreffend.
- **Source IP (IP-Quelladresse)**: Die IP-Adresse des Ausgangsgeräts für diesen Protokolleintrag
- **Quellport und -schnittstelle**: Die Portnummer des Dienstes des Ausgangsgeräts und ob es sich im LAN oder im WAN befand.
- **Ziel**: Der Name oder die IP-Adresse des Zielgeräts oder der Zielwebseite.
- **Zielport und -schnittstelle**: Die Portnummer des Dienstes des Zielgeräts und ob es sich im LAN oder im WAN befindet.

Erweiterte Einstellungen

6

In diesem Kapitel werden die erweiterten Funktionen des Routers beschrieben. Diese Informationen eignen sich für Benutzer mit fortgeschrittenen Netzwerkkenntnissen, die den Router für besondere Situationen konfigurieren möchten, etwa wenn Remote-Zugriff über das Internet über IP oder Domainnamen benötigt wird.

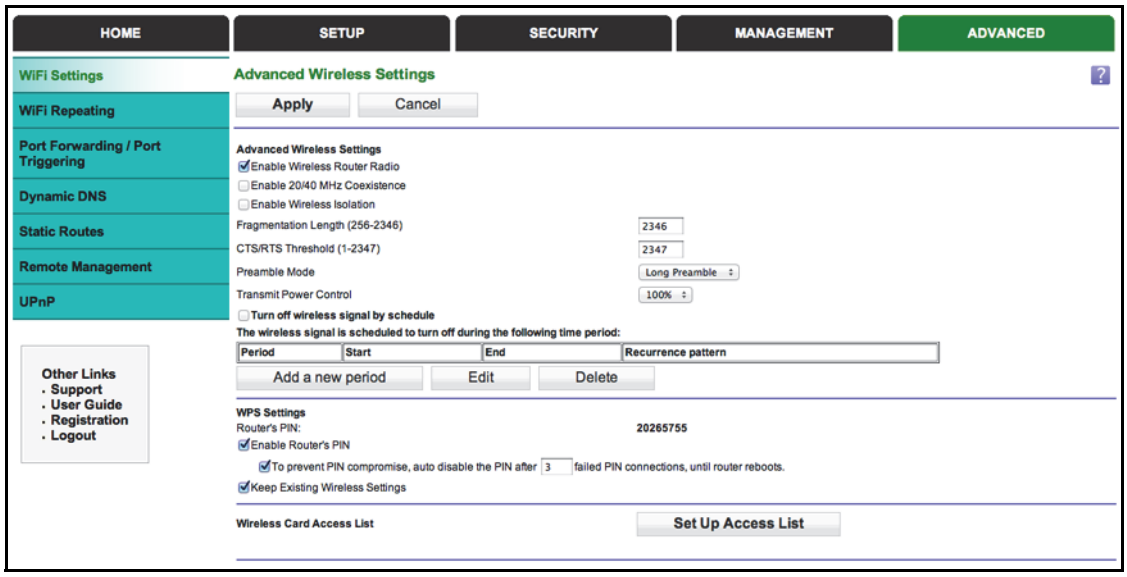
> **Hinweis:** Informationen zu Portweiterleitung und Port-Triggering finden Sie unter *Kapitel 4, Sicherheitseinstellungen*.

Dieses Kapitel enthält die folgenden Abschnitte:

- *Erweiterte WLAN-Konfiguration*
- *WLAN-Repeating (WDS)*
- *Dynamisches DNS*
- *Statische Routen*
- *Fernsteuerung*
- *Universal Plug and Play*

Erweiterte WLAN-Konfiguration

Wählen Sie **Advanced** (Erweitert) > **WiFi Settings** (WLAN-Konfiguration). Der folgende Bildschirm wird angezeigt:



Dieser Bildschirm enthält die folgenden Einstellungen:

Enable Wireless Router Radio (WLAN-Funktionen des Routers aktivieren): Sie können die WLAN-Funktionen des WLAN-Routers vollständig deaktivieren, indem Sie dieses Kontrollkästchen deaktivieren. Aktivieren Sie das Kontrollkästchen, wenn Sie die WLAN-Funktionen des Routers wieder aktivieren möchten. Wenn das WLAN deaktiviert ist, können andere Mitglieder des Haushalts den Router verwenden, indem sie ihre Computer mit einem Netzwerkkabel an den Router anschließen.

> **Hinweis:** Die Optionen **Fragmentation Length** (Fragmentierungsgrenzwert), **CTS/RTS Threshold** (CTS/RTS-Grenzwert) und **Preamble Mode** (Präambelmodus) dienen nur zum Testen des WLAN und der erweiterten Konfiguration. Nehmen Sie keine Änderungen an diesen Einstellungen vor.

Turn off wireless signal by schedule (WLAN-Signal nach Zeitplan abschalten): Mit dieser Funktion können Sie das WLAN-Signal des Routers zu Zeiten, an denen Sie keine WLAN-Verbindung benötigen, abschalten. Beispielsweise können Sie es für das Wochenende deaktivieren, wenn Sie verreisen.

WPS Settings (WPS-Einstellungen): Sie können dem Netzwerk WPS-Geräte hinzufügen.

Wireless Card Access List (Liste der zugriffsberechtigten WLAN-Karten): Klicken Sie auf die Schaltfläche **Set Up Access List** (Zugriffsliste anpassen), um den Bildschirm "Wireless

Card Access List" (Liste der zugriffsberechtigten WLAN-Karten) anzuzeigen. Sie können den Netzwerkzugriff auf einzelne Geräte mit vorgegebenen MAC-Adressen beschränken.

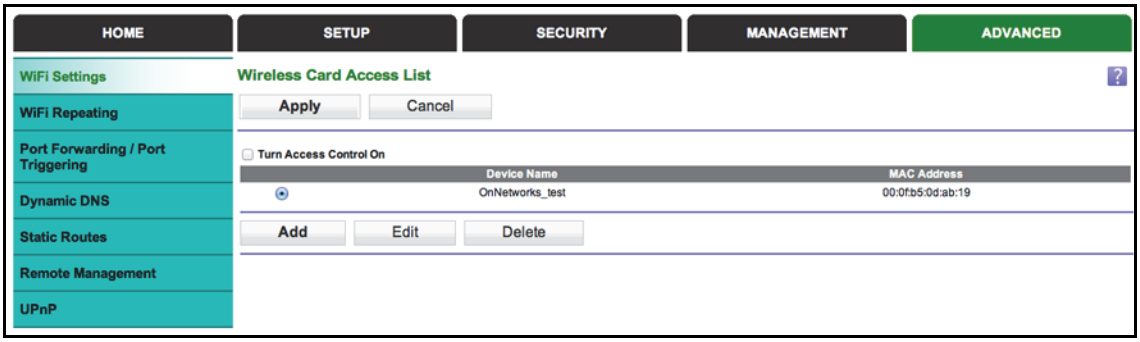
Einschränkung des WLAN-Zugriffs über MAC-Adressen

Sie haben die Möglichkeit, eine Liste der Computer und Wireless-Geräte zu erstellen, die eine Verbindung mit dem WLAN-Netzwerk herstellen können. Grundlage dieser Liste ist die eindeutige MAC-Adresse der Computer und Geräte.

Jedes Netzwerkgerät verfügt über eine MAC-Adresse, die aus einer eindeutigen physischen Adresse aus 12 Zeichen besteht, nur die Hexadezimalzeichen 0-9, a-f oder A-F enthalten kann und Doppelpunkte als Trennzeichen verwendet (z. B. 00:09:AB:CD:EF:01). Normalerweise wird die MAC-Adresse auf dem Typenschild der WLAN-Karte oder des Netzabschlussgeräts angegeben. Wenn das Typenschild nicht zugänglich ist, können Sie die MAC-Adresse über die Dienstprogramme der Netzwerkkonfiguration des Computers anzeigen. Möglicherweise finden Sie die MAC-Adressen auch im Bildschirm **Attached Devices** (Angeschlossene Geräte).

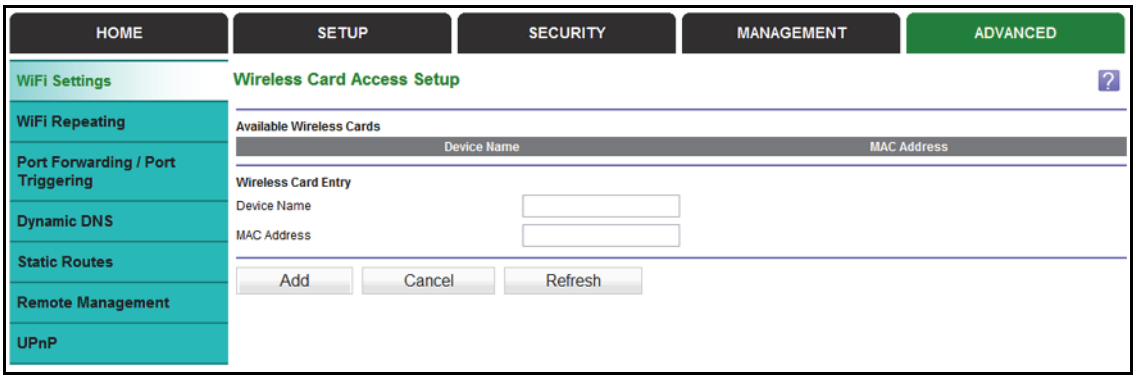
➢ **So schränken Sie den Zugriff anhand der MAC-Adressen ein:**

1. Wählen Sie **Advanced** (Erweitert) > **WiFi Setting** (WLAN-Konfiguration), und klicken Sie auf **Setup Access List** (Zugriffsliste anpassen), um die Liste der zugriffsberechtigten WLAN-Karten anzuzeigen.



2. Klicken Sie auf **Add** (Hinzufügen), um ein Wireless-Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen.

   Der Bildschirm **Wireless Card Access Setup** (WLAN-Karten einrichten) wird geöffnet. Er enthält eine Liste der aktuell aktiven WLAN-Karten mit den zugehörigen MAC-Adressen.



3. Wenn sich der gewünschte Computer oder das gewünschte Gerät in der Liste **Available Wireless Cards** (Verfügbare WLAN-Karten) befindet, aktivieren Sie die entsprechende Optionsschaltfläche. Geben Sie andernfalls einen Namen und die MAC-Adresse ein. Normalerweise wird die MAC-Adresse auf der Unterseite des Wireless-Geräts angegeben.

   Tipp: Sie können die MAC-Adressen vom Bildschirm **Attached Devices** (Angeschlossene Geräte) des Routers kopieren und in das MAC-Adressfeld dieses Bildschirms einfügen. Stellen Sie dazu von jedem WLAN-Computer eine Verbindung mit dem WLAN-Netzwerk her. Der Computer sollte nun im Bildschirm **Attached Devices** (Angeschlossene Geräte) angezeigt werden.

4. Klicken Sie auf **Add** (Hinzufügen), um dieses Wireless-Gerät in die Liste der zugriffsberechtigten WLAN-Karten aufzunehmen. Der Bildschirm wechselt nun wieder zum Listenbildschirm.
5. Fügen Sie alle Computer oder Geräte hinzu, die eine WLAN-Verbindung herstellen sollen.
6. Aktivieren Sie das Kontrollkästchen **Turn Access Control On** (Zugriffssteuerung aktivieren).
7. Klicken Sie auf **Apply** (Übernehmen).

WLAN-Repeating (WDS)

Sie können den N150R-Router als Wireless Access Point (AP) konfigurieren. Dadurch übernimmt der Router die Rolle eines WLAN-Repeaters. Ein WLAN-Repeater verbindet sich als Client mit einem anderen WLAN-Router, wobei das Netzwerk, mit dem die Verbindung besteht, den ISP-Dienst darstellt.

WLAN-Repeating ist eine Art WDS (Wireless Distribution System): Ein WDS ermöglicht es einem WLAN, seine Reichweite über mehrere Access Points zu erweitern, ohne dass zusätzliche Kabel für die Verbindung gelegt werden müssen. In der folgenden Abbildung wird ein WLAN-Repeating-Szenario dargestellt.

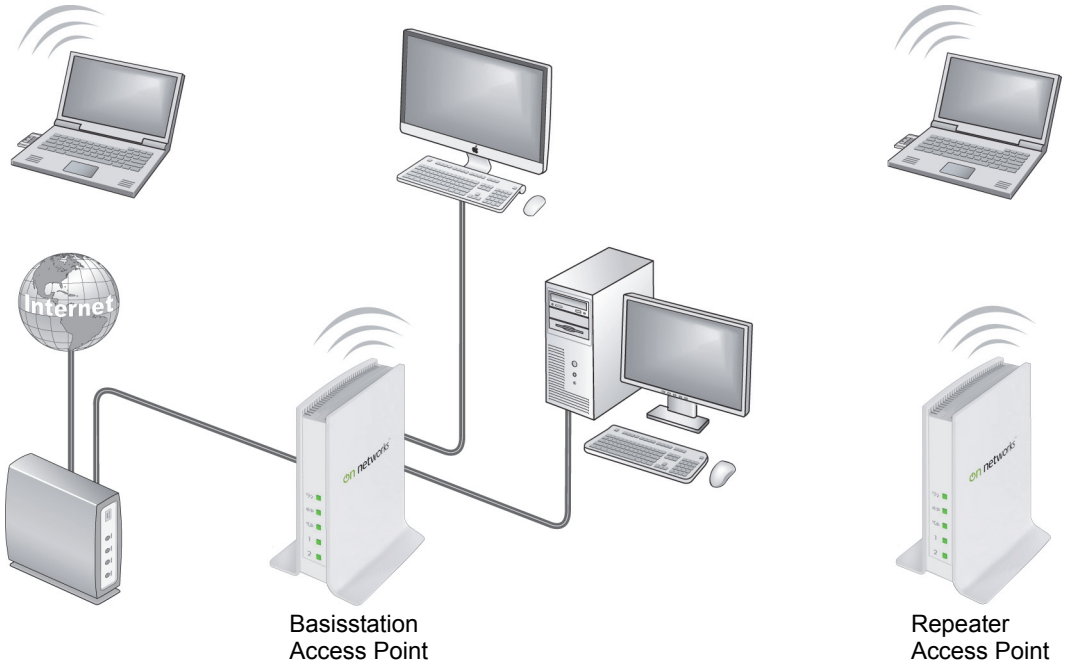


Abbildung 7. WLAN-Repeating-Szenario

Bei Verwendung der WLAN-Repeating-Funktion müssen Sie als Sicherheitsoption entweder WEP oder None (Keine) im Bildschirm **Wireless Settings** (WLAN-Konfiguration) auswählen. Die WEP-Option wird nur dann angezeigt, wenn Sie als WLAN-Modus im Bildschirm **Wireless Settings** (WLAN-Konfiguration) die Option Up to 54 Mbps (Bis zu 54 MBit/s) ausgewählt haben.

Wireless Base Station (WLAN-Basisstation): Der Router fungiert als übergeordneter Access Point, der den Datenverkehr zum und vom untergeordneten Repeater Access Point weiterleitet. Die Basisstation verwaltet zudem die über WLAN und Kabel verbundenen lokalen Computer. Zur Konfiguration dieses Modus benötigen Sie die MAC-Adressen des untergeordneten Repeater Access Points.

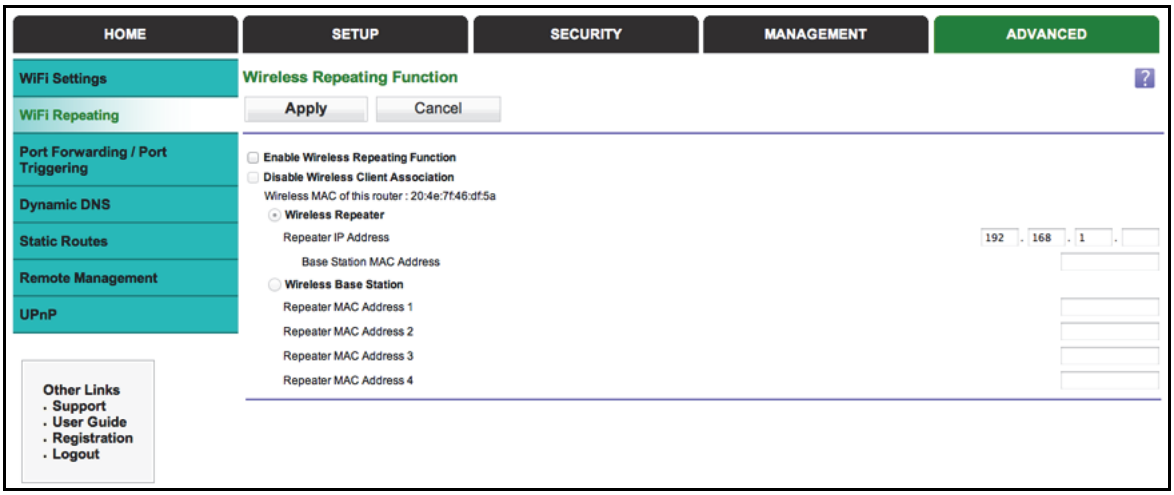
Wireless Repeater (WLAN-Repeater): Der Router sendet den gesamten Datenverkehr von den über WLAN und Kabel verbundenen Computern zu einem Remote Access Point. Zur Konfiguration dieses Modus benötigen Sie die MAC-Adresse des übergeordneten Remote Access Points.

Damit Sie ein WLAN mit WDS konfigurieren können, müssen die folgenden Bedingungen für beide Access Points erfüllt sein:

- Beide Access Points müssen dieselbe SSID, denselben Funkkanal und denselben Verschlüsselungsmodus verwenden.
- Beide Access Points müssen sich im selben LAN-IP-Subnetz befinden. Das bedeutet, die LAN-IP-Adressen des Access Points müssen sich im selben Netzwerk befinden.
- Alle LAN-Geräte (über WLAN und Kabel mit dem Netzwerk verbundene Computer) sind für den Betrieb im selben LAN-Netzwerkadressbereich wie die Access Points konfiguriert.

WLAN-Repeating

Wählen Sie **Advanced** (Erweitert) > **WiFi Repeating** (WLAN-Repeating) aus, um die WLAN-Repeater-Einstellungen des Routers anzuzeigen oder zu ändern.



- **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren): Aktivieren Sie dieses Kontrollkästchen, um WLAN-Repeating zu verwenden.

  Disable Wireless Client Association (WLAN-Client-Zuordnung deaktivieren): Wenn der Router die Rolle des Repeaters übernimmt, führt die Aktivierung dieses Kontrollkästchens dazu, dass die WLAN-Clients sich nicht verbinden können. Nur LAN-Client-Zuordnungen sind zulässig.

  - Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Punkt-zu-Punkt-Verbindung konfigurieren.
  - Aktivieren Sie dieses Kontrollkästchen dagegen nicht, wenn der gesamte Client-Datenverkehr über den anderen Access Point (Repeater mit WLAN-Client-Zuordnung) weitergeleitet werden soll.

- **Wireless MAC of this Router** (WLAN-MAC-Adresse dieses Routers): In diesem Feld wird die MAC-Adresse des Routers zu Ihrer Information angezeigt. Sie müssen die MAC-Adresse in den entsprechenden Bildschirm für das WLAN-Repeating des anderen verwendeten Access Points eingeben.
- **Wireless Repeater** (WLAN-Repeater): Aktivieren Sie dieses Kontrollkästchen, wenn der Router die Rolle des Repeaters übernimmt.

  Repeater IP Address (Repeater-IP-Adresse): Geben Sie die IP-Adresse des anderen Access Points ein, wenn der Router die Rolle des Repeaters übernimmt.

  Base Station MAC Address (MAC-Adresse der Basisstation): Geben Sie die MAC-Adresse des Access Points ein, der als Basisstation dient, wenn der Router die Rolle des Repeaters übernimmt.
- **Wireless Base Station** (WLAN-Basisstation): Aktivieren Sie dieses Kontrollkästchen, wenn der Router die Rolle der Basisstation übernimmt.

  Disable Wireless Client Association (WLAN-Client-Zuordnung deaktivieren): Wenn der Router die Rolle der Basisstation übernimmt, führt die Aktivierung dieses Kontrollkästchens dazu, dass die WLAN-Clients sich nicht verbinden können. Nur LAN-Client-Zuordnungen sind zulässig.

  Repeater MAC Address (Repeater-MAC-Adresse), 1 bis 4: Wenn der Router die Rolle der Basisstation übernimmt, kann er als „übergeordnete Instanz“ für bis zu 4 weitere Access Points fungieren. Geben Sie die MAC-Adressen der anderen Access Points in diese Felder ein.

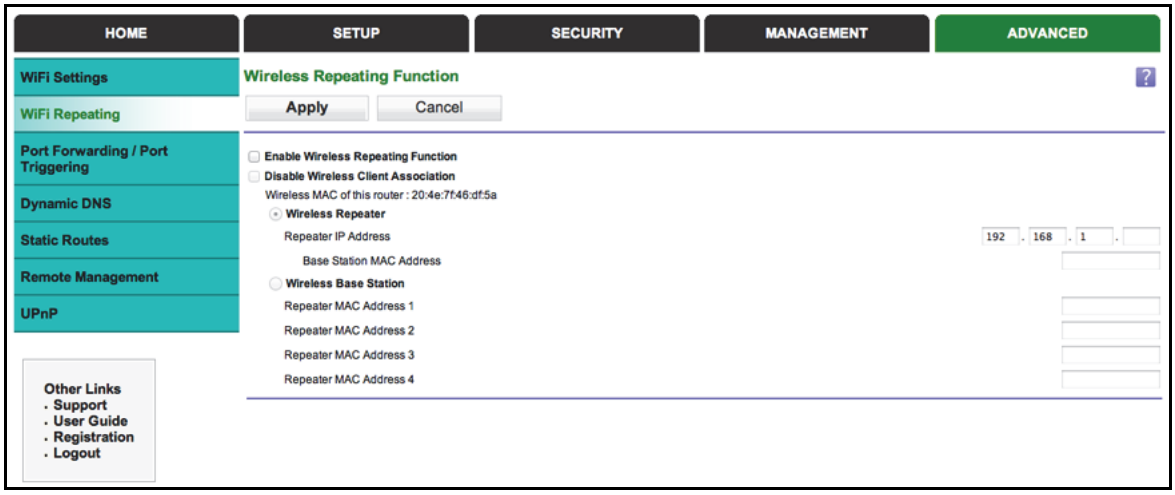
Konfigurieren der Basisstation

WLAN-Repeating kann nur in einer Speichenarchitektur verwendet werden. Die einzelnen Geräte können nicht in einer Daisy Chain in Serie miteinander verbunden werden. Sie benötigen dazu die WLAN-Einstellungen von beiden Geräten. Außerdem müssen Sie die MAC-Adresse des Remote-Geräts kennen. Konfigurieren Sie zuerst die Basisstation und danach den Repeater.

➢ **So konfigurieren Sie die Basisstation:**

1. Konfigurieren Sie beide Geräte mit denselben WLAN-Einstellungen (SSID, Modus, Kanal und Sicherheitsoption). Als WLAN-Sicherheitsoption muss **None** (Keine) oder **WEP** ausgewählt werden.

2. Wählen Sie **Advanced** (Erweitert) > **WiFi Repeating** (WLAN-Repeating) aus, um den Bildschirm **Wireless Repeating Function** (WLAN-Repeating) anzuzeigen.



3. Aktivieren Sie im Bildschirm **Wireless Repeating Function** (WLAN-Repeating) das Kontrollkästchen **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren), und wählen Sie die Optionsschaltfläche **Wireless Base Station** (WLAN-Basisstation).
4. Geben Sie die MAC-Adresse von einem oder mehreren Repeatern ein.
5. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).

Konfigurieren eines Repeaters

Konfigurieren Sie den Repeater über eine kabelgebundene Netzwerkverbindung, um Konflikte mit der WLAN-Verbindung zur Basisstation zu vermeiden.

> **Hinweis:** Wenn Sie die N150R-Basisstation mit einem Router einer anderen Marke als der des Repeaters verwenden, müssen Sie möglicherweise weitere Konfigurationseinstellungen ändern. Insbesondere sollten Sie die DHCP-Serverfunktion des Wireless Repeater APs deaktivieren.

➢ **So konfigurieren Sie den Router als Repeater:**

1. Melden Sie sich bei dem Router an, der die Rolle des Repeaters übernimmt. Wählen Sie **Setup** (Konfiguration) > **WiFi Settings** (WLAN-Konfiguration) aus, und stellen Sie sicher, dass die WLAN-Einstellungen vollständig mit denen der Basisstation übereinstimmen. Als WLAN-Sicherheitsoption muss **WEP** oder **None** (Keine) ausgewählt sein.
2. Wählen Sie **Advanced** (Erweitert) > **WiFi Repeating Function** (WLAN-Repeating) und aktivieren Sie das Kontrollkästchen **Enable Wireless Repeating Function** (WLAN-Repeating aktivieren) und die Optionsschaltfläche **Wireless Repeater** (WLAN-Repeater).

3. Füllen Sie das Feld für die Repeater-IP-Adresse aus. Diese IP-Adresse muss sich im selben Subnetz wie die Basisstation befinden, jedoch von der LAN-IP-Adresse der Basisstation unterscheiden.
4. Klicken Sie zum Speichern der Änderungen auf **Apply** (Übernehmen).
5. Prüfen Sie die Verbindungen in den LANs.

   Ein Computer in einem beliebigen WLAN- oder kabelgebundenen LAN-Segment des Routers muss eine Verbindung mit dem Internet herstellen oder Dateien und Drucker für alle anderen über WLAN oder Kabel verbundenen Computer oder Server, die mit dem anderen Access Point verbunden sind, freigeben können.

Dynamisches DNS

Wenn Ihr ISP (Internet-Provider) Ihrem Netzwerk eine permanente IP-Adresse zugewiesen hat, können Sie einen Domainnamen registrieren und diesen Namen über öffentliche Domain Name Server (DNS) mit Ihrer IP-Adresse verknüpfen lassen. Falls Ihr Internetzugang jedoch über dynamisch vergebene IP-Adressen funktioniert, können Sie nicht im Voraus sagen, wie Ihre IP-Adresse lauten wird. Zudem kann die Adresse sich häufig ändern. In diesem Fall können Sie einen kommerziellen dynamischen DNS-Dienst nutzen. Bei diesem Diensttyp können Sie Ihre Domain unter der IP-Adresse dieses Anbieters registrieren und für Ihre Domain bestimmten Datenverkehr an Ihre aktuelle IP-Adresse weiterleiten lassen.

Wenn Ihr ISP private WAN-IP-Adressen vergibt (wie z. B. 192.168.x.x oder 10.x.x.x), funktioniert der dynamische DNS-Dienst nicht, da eine Internet-Weiterleitung an private Adressen nicht möglich ist.

Der Router enthält einen Client, der eine Verbindung mit dem von DynDNS.org bereitgestellten dynamischen DNS-Dienst herstellen kann. Besuchen Sie zuerst die Website unter *http://www.dyndns.org*, und legen Sie ein Konto und einen Hostnamen an, den Sie im Router konfigurieren. Sobald sich die vom ISP zugewiesene IP-Adresse ändert, kontaktiert Ihr Router automatisch den Anbieter des dynamischen DNS-Diensts, meldet sich bei Ihrem Konto an und registriert die neue IP-Adresse. Falls Ihr Hostname beispielsweise **hostname** lautet, können Sie den Router unter *http://hostname.dyndns.org* erreichen.

Wählen Sie **Advanced** (Erweitert) > **Dynamic DNS** (Dynamischer DNS-Dienst). Der folgende Bildschirm wird angezeigt:

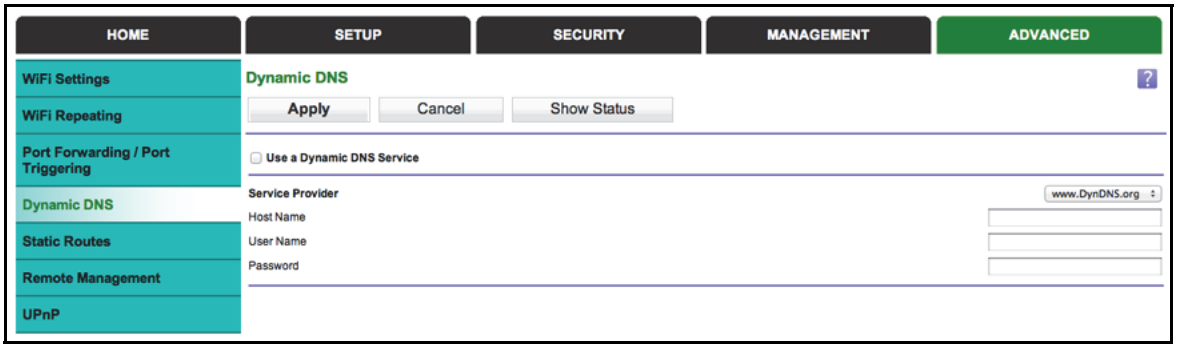


Abbildung 8. Weiterleiten des Datenverkehrs an eine wechselnde IP-Adresse

➢ **So konfigurieren Sie dynamisches DNS:**

1. Richten Sie ein Konto bei einem der Anbieter für dynamische DNS-Dienste ein, die in der Liste **Service Provider** (Dienstanbieter) angezeigt werden. Wählen Sie für DynDNS.org etwa *www.dyndns.org* aus.
2. Aktivieren Sie das Kontrollkästchen **Use a Dynamic DNS Service** (DDNS-Dienst verwenden).
3. Wählen Sie den Namen Ihres DDNS-Anbieters aus.
4. Geben Sie den Hostnamen (oder Domainnamen) ein, der Ihnen vom DDNS-Anbieter zugewiesen wurde.
5. Geben Sie den Benutzernamen für Ihr DDNS-Konto ein. Dabei handelt es sich um den Namen für die Anmeldung bei Ihrem Konto, nicht um Ihren Hostnamen.
6. Geben Sie das Passwort (oder den Schlüssel) für Ihr DDNS-Konto ein.
7. Wenn Ihr DDNS-Anbieter für die Auflösung Ihrer URL die Verwendung von Platzhaltern zulässt, können Sie zur Aktivierung dieser Funktion das Kontrollkästchen **Use Wildcards** (Platzhalter verwenden) aktivieren.

   Die Platzhalter-Funktion ermöglicht es z. B., dass **.ihrhost.dyndns.org* als Alias für dieselbe IP-Adresse wie **ihrhost.dyndns.org** akzeptiert wird.
8. Klicken Sie auf **Apply** (Übernehmen).

Statische Routen

Statische Routen liefern Ihrem Router zusätzliche Routinginformationen. In der Regel müssen Sie keine statischen Routen hinzufügen. Statische Routen müssen nur in Ausnahmefällen festgelegt werden, z. B. wenn Ihr Netzwerk mehrere Router oder IP-Subnetze enthält.

Im Folgenden finden Sie ein Beispiel für einen Fall, der den Einsatz einer statischen Route erforderlich macht:

- Ihr Hauptinternetzugang erfolgt über ein Kabelmodem, das Sie mit dem Internet-Provider verbindet.
- Außerdem ist an Ihr Heimnetzwerk ein ISDN-Router angeschlossen, über den Sie eine Verbindung zu dem Unternehmen, für das Sie arbeiten, aufbauen. Die Adresse dieses Routers in Ihrem LAN lautet 192.168.1.100.
- Die Netzwerkadresse des Unternehmens ist 134.177.0.0.

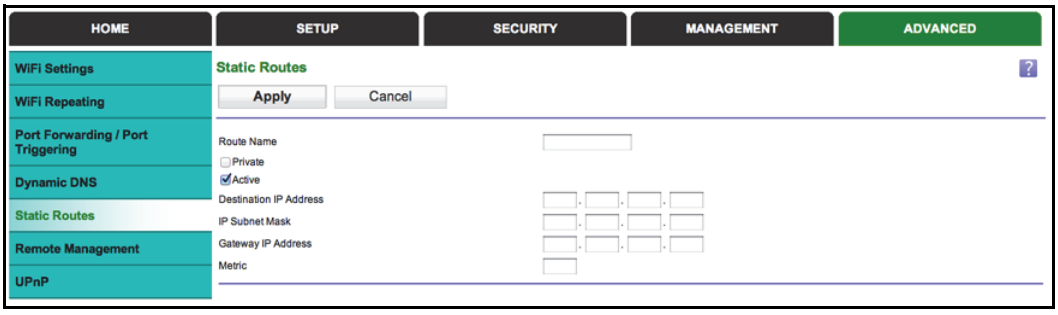
Bei der Anfangskonfiguration des Routers wurden zwei statische Routen erstellt. Es wurde eine Standardroute mit Ihrem Internet-Provider als Gateway eingerichtet sowie eine zweite statische Route zu Ihrem lokalen Netzwerk für sämtliche Adressen des Typs 192.168.1.x. Wenn Sie versuchen, mit dieser Konfiguration auf ein Gerät im Netzwerk 134.177.0.0 zuzugreifen, leitet Ihr Router diese Anforderung an den ISP weiter. Der ISP gibt diese Anforderung an das Unternehmen, für das Sie arbeiten, weiter, wo sie wahrscheinlich von der Unternehmensfirewall abgelehnt wird.

In diesem Fall müssen Sie eine statische Route festlegen, die den Router dazu veranlasst, über den ISDN-Router mit der Adresse 192.168.1.100 auf die Adresse 134.177.0.0 zuzugreifen. In diesem Beispiel gilt:

- Die Einträge in den Feldern **Destination IP Address** (IP-Zieladresse) und **IP Subnet Mask** (IP-Subnetzmaske) legen fest, dass diese statische Route für alle Adressen des Typs 134.177.x.x gilt.
- Der Wert im Feld **Gateway IP Address** (Gateway-IP-Adresse) gibt an, dass der gesamte Datenverkehr für diese Adressen an den ISDN-Router mit der Adresse 192.168.1.100 weitergeleitet werden soll.
- Im Feld **Metric** (Metrik) kann **1** stehen, da der ISDN-Router sich innerhalb des LANs befindet.
- **Privat** wurde nur als Vorsichtsmaßnahme ausgewählt, falls RIP aktiviert ist.

➢ **So konfigurieren Sie eine statische Route:**

1. Wählen Sie **Advanced** (Erweitert) > **Static Routes** (Statische Routen) aus, und klicken Sie auf **Add** (Hinzufügen), um den folgenden Bildschirm anzuzeigen:



2. Geben Sie in das Feld **Route Name** (Routenname) einen Namen für diese statische Route ein (nur zu Identifikationszwecken).
3. Aktivieren Sie das Kontrollkästchen **Private** (Privat), wenn Sie den Zugriff auf das LAN beschränken möchten. Bei Aktivierung der Option **Private** (Privat) wird die statische Route nicht im RIP angegeben.
4. Aktivieren Sie das Kontrollkästchen **Active** (Aktiv), um diese Route zu aktivieren.

5. Geben Sie die IP-Zieladresse des Zielhosts für die Route ein.
6. Geben Sie die IP-Subnetzmaske für das Ziel ein. Wenn es sich dabei um einen einzelnen Host handelt, geben Sie **255.255.255.255** als Ziel ein.
7. Geben Sie die Gateway-IP-Adresse ein; hierbei muss es sich um einen Router im selben LAN-Segment wie der N150R-Router handeln.
8. Geben Sie im Feld **Metric** (Metrik) einen Wert aus dem Bereich 1 bis 15 ein.

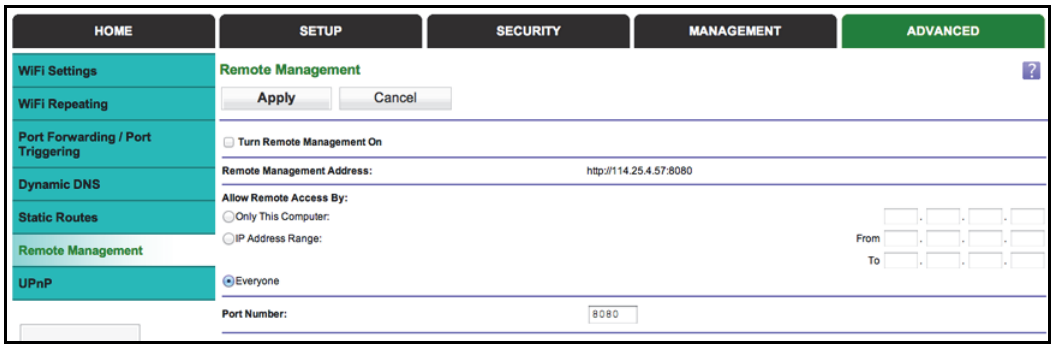
   Dieser Wert steht für die Anzahl der Router zwischen Ihrem Netzwerk und dem Ziel. In der Regel funktionieren die Werte 2 und 3; bei direkten Verbindungen sollte jedoch immer der Wert 1 gewählt werden.
9. Klicken Sie auf **Apply** (Übernehmen), um die statische Route hinzuzufügen.

Fernsteuerung

Mit der Fernsteuerung können Sie den Status des N150R-Routers über das Internet aktualisieren oder prüfen.

➢ **So richten Sie die Fernsteuerung ein:**

1. Wählen Sie **Advanced** (Erweitert) > **Remote Management** (Fernsteuerung) aus.



Hinweis: *Ersetzen Sie das Standard-Anmeldepasswort des Routers unbedingt durch ein sicheres Passwort. Das ideale Passwort enthält keine Wörter aus Wörterbüchern jeglicher Sprache und besteht aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen. Es kann aus bis zu 30 Zeichen bestehen.*

2. Aktivieren Sie das Kontrollkästchen **Turn Remote Management On** (Fernsteuerung aktivieren).
3. Geben Sie unter "Allow Remote Access By" (Remote-Zugriff zulassen) die externen IP-Adressen an, die auf die Router-Fernsteuerung zugreifen können.

Hinweis: Aus Sicherheitsgründen sollte der Fernzugriff auf einige wenige externe IP-Adressen beschränkt bleiben.

- Wenn nur eine einzige IP-Adresse im Internet die Zugriffsrechte erhalten soll, wählen Sie **Only This Computer** (Nur für diesen Computer). Geben Sie die IP-Adresse ein, die die Zugriffsrechte erhalten soll.
- Wenn nur IP-Adressen eines bestimmten Bereichs Zugriffsrechte erhalten sollen, wählen Sie **IP Address Range** (IP-Adressbereich). Geben Sie eine erste und eine letzte IP-Adresse ein, um den Bereich erlaubter Adressen festzulegen.
- Um die IP-Adressen anzugeben, wählen Sie **IP Address List** (IP-Adressliste) aus, und geben Sie die zulässigen IP-Adressen ein.
- Wenn jede beliebige IP-Adresse im Internet Zugriffsrechte erhalten soll, wählen Sie **Everyone** (Uneingeschränkt).

4. Geben Sie die Portnummer für den Zugriff auf die Fernsteuerungsoberfläche an.

   Dem normalen Zugriff über einen Webbrowser ist der Standard-HTTP-Dienstport 80 zugewiesen. Zur Erhöhung der Sicherheit können Sie eine benutzerdefinierte Portnummer für den Fernzugriff per Internet auf den Router eingeben. Wählen Sie eine Nummer im Bereich 1024 bis 65535. Verwenden Sie jedoch keine Standard-Portnummern gängiger Internetdienste. Als Standardwert ist 8080 eingestellt, ein gängiges Alias für HTTP.

5. Klicken Sie auf **Apply** (Übernehmen), um die Änderungen an den Router zu übermitteln.
6. Um über das Internet auf den Router zugreifen zu können, müssen Sie die WAN-IP-Adresse des Routers in die Adressleiste des Webbrowsers eingeben, gefolgt von einem Doppelpunkt (:) und der benutzerdefinierten Portnummer. Angenommen, die derzeitige externe IP-Adresse Ihres Routers lautet 134.177.0.123 und Sie verwenden Portnummer 8080. Dann müssen Sie im Browser **http://134.177.0.123:8080** eingeben.

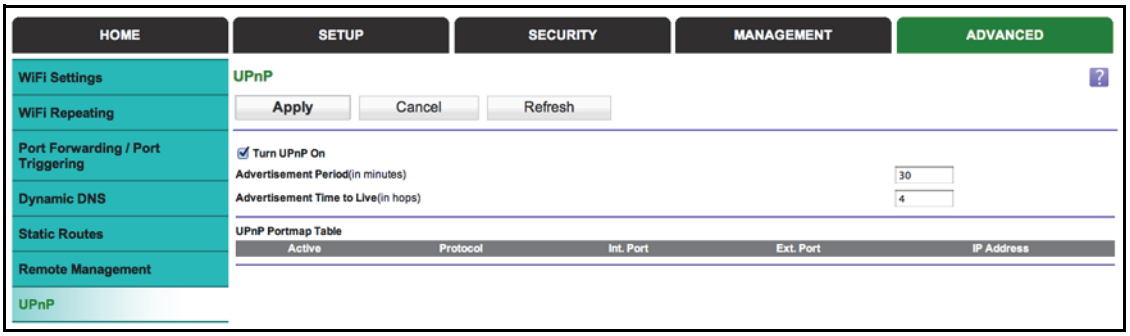
Universal Plug and Play

Universal Plug and Play (UPnP) vereinfacht den Netzwerkzugriff und die Vernetzung von Geräten aller Art, beispielsweise von Internet-Geräten und Computern. UPnP-fähige Geräte erkennen die von anderen registrierten UPnP-Geräten im Netzwerk angebotenen Dienste automatisch.

Wenn Sie Anwendungen wie Multi-Player-Games, Peer-to-Peer-Verbindungen und Echtzeitkommunikation (z. B. Instant Messaging oder die Remoteunterstützung von Windows XP) verwenden, sollten Sie UPnP aktivieren.

➢ **So aktivieren Sie Universal Plug and Play:**

1. Wählen Sie **Advanced** (Erweitert) > **UPnP** aus. Der Bildschirm **UPnP** wird angezeigt.



2. Auf diesem Bildschirm sind die folgenden Einstellungen und Informationen verfügbar:

   Turn UPnP On (UPnP aktivieren): Die automatische Gerätekonfiguration per UPnP kann aktiviert oder deaktiviert werden. Standardmäßig ist UPnP deaktiviert. Wenn dieses Kontrollkästchen nicht aktiviert ist, lässt der Router nicht zu, dass andere Geräte die Ressourcen des Routers (wie z. B. die Portweiterleitung/Portzuordnung) automatisch steuern.

   Advertisement Period (Advertising-Periode): Die Advertising-Periode bestimmt, wie oft die UPnP-Daten des Routers per Broadcast gesendet werden. Hier können Werte im Bereich 1 bis 1440 Minuten angegeben werden. Der Standardwert ist 30 Minuten. Kürzere Perioden stellen sicher, dass die Steuerungspunkte über aktuelle Informationen zum Gerätestatus verfügen, führen jedoch zu einem erhöhten Datenverkehr im Netzwerk. Bei längeren Perioden werden die Gerätestatusinformationen weniger oft aktualisiert; dafür verringert sich jedoch der Datenverkehr im Netzwerk erheblich.

   Advertisement Time to Live (Advertising-Lebensdauer): Die Advertising-Lebensdauer wird in Hops (Schritten) für jedes gesendete UPnP-Paket gemessen. Die Lebensdauer gibt die maximale Anzahl von Hops für die Weitergabe eines Broadcast-Pakets beim UPnP-Advertising an. Für die Anzahl der Hops können Werte im Bereich 1 bis 255 angegeben werden. Der Standardwert für die Advertising-Lebensdauer ist 4 Hops. Für Netzwerke in Privathaushalten ist dieser Wert in der Regel ausreichend. Wenn Sie feststellen, dass einige Geräte nicht aktualisiert oder nicht erreicht werden, sollten Sie einen höheren Wert wählen.

   UPnP Portmap Table (UPnP-Portzuordnungstabelle): In der UPnP-Portzuordnungstabelle werden die IP-Adressen aller aktuell auf den Router zugreifenden UPnP-Geräte und die von diesen geöffneten Ports (intern und extern) angezeigt. Darüber hinaus können Sie der UPnP-Portzuordnungstabelle die Typen der geöffneten Ports und deren Status (d. h. ob diese für die einzelnen IP-Adressen noch aktiv sind) entnehmen.

3. Klicken Sie auf **Apply** (Übernehmen), um die Einstellungen zu speichern.

Fehlerbehebung

7

Diagnostizieren und Lösen von Problemen

In diesem Kapitel finden Sie Informationen zur Behebung von Fehlern bei Ihrem N150 WLAN-Router (N150R). Nach der Beschreibung eines Problems finden Sie jeweils eine Anleitung zur Diagnose und Behebung des Problems.

Tipp: On Networks stellt hilfreiche Artikel, Dokumentationen und die aktuellen Softwareaktualisierungen unter *http://www.on-networks.com/support* bereit.

Dieses Kapitel enthält die folgenden Abschnitte:

- *Tipps*
- *Behebung von Fehlern im Zusammenhang mit LEDs*
- *Anmeldung am Router nicht möglich*
- *Es kann keine Internetverbindung hergestellt werden*
- *Änderungen werden nicht gespeichert*
- *Verbindung über WLAN*
- *Wiederherstellen der Werkseinstellungen und des Passworts*
- *Fehlerbehebung im Netzwerk mithilfe des Ping-Dienstprogramms*

Tipps

In diesem Abschnitt erhalten Sie Tipps zur Behebung häufiger Probleme.

Sequenz zum Neustart des Netzwerks

Führen Sie die folgenden Schritte aus, wenn Sie das Netzwerk neu starten müssen:

1. Schalten Sie das Modem aus *und* ziehen Sie den Netzstecker.
2. Schalten Sie den Router und die Computer aus.
3. Schließen Sie das Modem an, und schalten Sie es ein. Warten Sie 2 Minuten.
4. Schalten Sie den Router ein, und warten Sie 2 Minuten.
5. Schalten Sie die Computer ein.

Überprüfen der Netzwerkkabel

Überprüfen Sie, ob die Netzwerkkabel richtig angeschlossen sind.

- Die Internet-LED des Routers leuchtet, wenn das Netzwerkkabel ordnungsgemäß mit dem Modem und dem Router verbunden ist und Modem und Router eingeschaltet sind.
- Für jeden eingeschalteten Computer, der über ein Netzwerkkabel mit dem Router verbunden ist, leuchtet die entsprechende nummerierte Status-LED des LAN-Ports am Router auf.

WLAN-Einstellungen

Wenn Sie Probleme mit dem Herstellen einer Verbindung mit dem WLAN-Netzwerk haben, stellen Sie sicher, dass die WLAN-Einstellungen auf dem Computer und Router genau übereinstimmen.

- Bei einem über WLAN verbundenen Computer müssen der WLAN-Netzwerkname (SSID) und die WLAN-Sicherheitseinstellungen des Routers und WLAN-Computers identisch sein.
- Wenn Sie eine Zugriffsliste auf dem Bildschirm **Advanced Wireless Settings** (Erweiterte WLAN-Konfiguration) einrichten, müssen Sie die MAC-Adressen aller über WLAN verbundenen Computer der Router-Zugriffsliste hinzufügen.

Netzwerkeinstellungen

Wenn Sie nicht auf das Netzwerk zugreifen können, stellen Sie sicher, dass die Netzwerkeinstellungen des Computers richtig sind.

- Die Netzwerk-IP-Adressen von über WLAN und Kabel angeschlossenen Computern müssen sich im selben Netzwerk wie der Router befinden. Die einfachste Möglichkeit dazu besteht darin, alle Computer so zu konfigurieren, dass sie automatisch eine IP-Adresse über DHCP beziehen.

- Bei manchen Kabelmodem-Anbietern müssen Sie die MAC-Adresse des Computers verwenden, der ursprünglich für Ihren Zugang registriert wurde. Sie können die MAC-Adresse auf dem Bildschirm **Attached Devices** (Angeschlossene Geräte) anzeigen.

Behebung von Fehlern im Zusammenhang mit LEDs

Nach dem Einschalten des Routers treten die folgenden Ereignisse in der angegebenen Reihenfolge auf:

1. Überprüfen Sie nach dem Einschalten, ob die Power-/Test-LED leuchtet.
2. Überprüfen Sie, ob die Power-/Test-LED nach einigen Sekunden beginnt, grün zu blinken. Sie zeigt an, dass ein Selbsttest durchgeführt wird.
3. Überprüfen Sie nach ca. 30 Sekunden Folgendes:
   - Die Power-/Test-LED leuchtet grün.
   - Die Internet-LED leuchtet.
   - Für jeden mit einem Computer verbundenen LAN-Port leuchtet eine nummerierte Netzwerkanschluss-LED. Dies bedeutet, dass eine Verbindung mit dem angeschlossenen Gerät besteht.

Die LED an der Vorderseite des Routers kann zur Problembehebung verwendet werden.

Die Power-/Test-LED ist aus

- Vergewissern Sie sich, dass das Stromkabel richtig mit dem Router verbunden ist und dass das Netzteil ordnungsgemäß an eine funktionierende Steckdose angeschlossen ist.
- Prüfen Sie, ob Sie das Netzteil verwenden, das im Lieferumfang des Produkts enthalten war.
- Wenn die Power-/Test-LED langsam und kontinuierlich blinkt, ist die Routerfirmware fehlerhaft. Dies kann vorkommen, wenn eine Firmware-Aktualisierung unterbrochen wird oder der Router ein Problem mit der Firmware erkennt. Falls sich der Fehler nicht beheben lässt, besteht ein Hardwareproblem. Wenden Sie sich an den technischen Support unter *http://www.on-networks.com/support*, um Informationen zur Wiederherstellung oder Hilfe bei einem Hardwareproblem zu erhalten.

Power-/Test-LED bleibt gelb

Beim Einschalten des Routers leuchtet die Power-/Test-LED für ungefähr 20 Sekunden gelb und wird dann grün. Leuchtet die LED nicht grün, liegt ein Routerfehler vor.

Wenn die Power-/Test-LED auch 1 Minute nach Einschalten der Stromzufuhr zum Router noch gelb leuchtet:

1. Schalten Sie das Gerät aus und wieder ein, um festzustellen, ob der Router wiederhergestellt wird.

2. Halten Sie die **Reset-Taste** gedrückt, um den Router auf die Werkseinstellungen zurückzusetzen. Dieser Vorgang wird unter *Wiederherstellen der Werkseinstellungen und des Passworts* auf Seite 89 erläutert.

Wenn der Fehler sich nicht beheben lässt, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support unter *http://www.on-networks.com/support*.

Die LEDs erlöschen nicht

Beim Einschalten des Routers leuchten die LEDs für ungefähr 10 Sekunden auf und erlöschen dann wieder. Wenn alle LEDs weiterleuchten, liegt ein Routerfehler vor.

Wenn sämtliche LEDs eine Minute nach Einschalten des Routers immer noch leuchten, sollten Sie die folgenden Schritte durchführen:

- Schalten Sie das Router aus und wieder ein, um zu sehen, ob der Fehler nur vorübergehend aufgetreten ist.
- Halten Sie die **Reset-Taste** gedrückt, um den Router auf die Werkseinstellungen zurückzusetzen. Dieser Vorgang wird unter *Wiederherstellen der Werkseinstellungen und des Passworts* auf Seite 89 erläutert.

Wenn der Fehler sich nicht beheben lässt, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support unter *http://www.on-networks.com/support*.

Die Internet- oder Netzwerkanschluss-LEDs leuchten nicht

Falls die Netzwerkanschluss-LEDs oder die Internet-LED nicht leuchten, wenn eine Netzwerkverbindung hergestellt wird, überprüfen Sie die folgenden Punkte:

- Das Netzwerkkabel muss fest in die Anschlüsse am Router und am Modem oder Computer eingesteckt sein.
- Das angeschlossene Modem bzw. der Computer muss eingeschaltet sein.
- Vergewissern Sie sich, dass das richtige Kabel verwendet wird:

  Stellen Sie die Verbindung zwischen Router-Internet-Port und Kabel- oder DSL-Modem mit dem Kabel her, das dem Modem beilag. Dieses Kabel kann ein handelsübliches Netzwerkkabel oder ein Crossover-Kabel sein.

Anmeldung am Router nicht möglich

Wenn Sie sich nicht über einen Computer im lokalen Netzwerk am Router anmelden können, überprüfen Sie die folgenden Punkte:

- Wenn Sie einen am Netzwerk angeschlossenen Computer verwenden, überprüfen Sie – wie im vorangehenden Abschnitt beschrieben – die Netzwerkverbindung zwischen dem Computer und dem Router.
- Vergewissern Sie sich, dass die IP-Adresse des Computers zum selben Subnetz gehört wie der Router. Wenn Sie das empfohlene Adressenschema verwenden, sollte die IP-Adresse des Computers im Bereich von 192.168.1.2 bis 192.168.1.254 liegen.

- Wird als IP-Adresse des Computers 169.254.x.x angezeigt, erstellen neuere Versionen von Windows und Mac OS eine IP-Adresse und weisen diese zu, wenn der Computer keinen DHCP-Server erreichen kann. Diese automatisch erstellten IP-Adressen liegen im Bereich 169.254.x.x. Wenn die IP-Adresse in diesem Bereich liegt, sollten Sie die Verbindung vom Computer zum Router überprüfen und den Computer neu starten.
- Wenn die IP-Adresse des Routers sich geändert hat und Sie die aktuelle IP-Adresse nicht kennen, setzen Sie die Konfiguration des Routers auf die werkseitigen Voreinstellungen zurück. Dabei wird als IP-Adresse des Routers 192.168.1.1 festgelegt. Eine Anleitung hierzu finden Sie unter *Werkseitige Voreinstellungen* auf Seite 93.
- Vergewissern Sie sich, dass bei Ihrem Browser Java, JavaScript und ActiveX aktiviert sind. Wenn Sie den Internet Explorer verwenden, klicken Sie auf **Aktualisieren**, um sicherzugehen, dass das Java-Applet geladen wurde.
- Schließen Sie den Browser, und starten Sie ihn erneut.
- Vergewissern Sie sich, dass Sie die korrekten Anmeldedaten verwenden. Die werkseitigen Voreinstellungen sind wie folgt: Der Benutzername lautet **admin** und das Passwort **admin**. Achten Sie darauf, dass beim Eingeben dieser Daten die Feststelltaste nicht aktiviert ist.
- Wenn Sie vorhaben, den Router als zusätzlichen Router hinter einem bestehenden Router in Ihrem Netzwerk einzurichten, sollten Sie in Erwägung ziehen, den bestehenden Router zu ersetzen.
- Wenn Sie diesen Router als Ersatz für einen ADSL-Modemrouter in Ihrem Netzwerk einrichten, kann der Router viele Gatewaydienste nicht ausführen. z. B. das Konvertieren von ADSL- oder Kabeldaten in Netzwerkdaten.

Es kann keine Internetverbindung hergestellt werden

Wenn Sie zwar auf den Router, jedoch nicht auf das Internet zugreifen können, überprüfen Sie zuerst, ob der Router eine IP-Adresse von Ihrem ISP (Internet-Provider) beziehen kann. Wurde Ihnen keine statische IP-Adresse vom ISP zugewiesen, fordert der Router eine IP-Adresse vom ISP an. Mithilfe des Bildschirms **Router Status** (Routerstatus) können Sie überprüfen, ob die Anforderung erfolgreich war.

➢ **So überprüfen Sie die WAN-IP-Adresse:**

1. Starten Sie den Browser, und besuchen Sie eine externe Website, z. B. **www.on-networks.com**.
2. Rufen Sie die -Benutzeroberfläche über **www.mywifirouter.com** auf.
3. Wählen Sie **Management** (Verwaltung) > **Router Status** (Routerstatus).
4. Prüfen Sie, ob eine IP-Adresse für den Internet-Port angezeigt wird. Wenn 0.0.0.0 angezeigt wird, konnte der Router keine IP-Adresse vom Internet-Provider abrufen.

Wenn Ihr Router keine IP-Adresse vom ISP beziehen kann, müssen Sie u. U. das Kabel- oder DSL-Modem zwingen, den neuen Router zu erkennen, indem Sie das Netzwerk neu starten. Dieser Vorgang wird unter *Sequenz zum Neustart des Netzwerks* auf Seite 82 erläutert.

Wenn der Router weiterhin keine IP-Adresse vom ISP beziehen kann, kann dies folgende Ursachen haben:

- Möglicherweise erfordert Ihr ISP ein Anmeldeprogramm.
  Erkundigen Sie sich beim ISP, ob Sie PPP over Ethernet (PPPoE) oder ein anderes Anmeldeprotokoll benötigen.
- Falls eine Anmeldung beim ISP erforderlich ist, sind der Benutzername und das Passwort zur Anmeldung möglicherweise falsch festgelegt.
- Der Provider überprüft vielleicht den Hostnamen des Computers.
  Geben Sie im Bildschirm **Internet Setup** (Internetkonfiguration) als Kontonamen den Computer-Hostnamen des Internetkontos ein.
- Der ISP erlaubt nur einer MAC-Adresse den Verbindungsaufbau zum Internet und überprüft die MAC-Adresse des Computers. Wählen Sie in diesem Fall eine der folgenden Optionen:
  - Teilen Sie dem ISP mit, dass Sie ein neues Netzwerkgerät erworben haben, und bitten Sie darum, die MAC-Adresse des Routers zu verwenden.
  - Konfigurieren Sie Ihren Router so, dass er die MAC-Adresse des Computers klont.

Wenn der Router eine IP-Adresse erhält, Sie aber dennoch keine Webseiten aus dem Internet anzeigen können, kann dies folgende Ursachen haben:

- Ihr Computer erkennt möglicherweise keine DNS-Serveradressen.

  Ein DNS-Server ist ein Host im Internet, der Internetnamen (z. B. www-Adressen) in numerische IP-Adressen umwandelt. Normalerweise stellt der ISP Ihnen die Adressen von einem oder zwei DNS-Servern automatisch zur Verfügung. Wenn Sie bei der Konfiguration des Routers eine DNS-Adresse eingegeben haben, starten Sie den Computer neu, und überprüfen Sie die DNS-Adresse. Sie können die DNS-Adressen manuell auf dem Computer konfigurieren. Informationen dazu finden Sie in der Dokumentation zu Ihrem Betriebssystem.
- Der Router ist auf dem Computer nicht als TCP/IP-Gateway konfiguriert.

  Wenn der Computer seine Daten über DHCP vom Router bezieht, starten Sie den Computer neu, und überprüfen Sie die Gateway-Adresse.
- Möglicherweise führen Sie für die Anmeldung eine Software aus, die nicht mehr benötigt wird.

  Wenn Ihnen der ISP ein Programm für die Anmeldung beim Internet zur Verfügung gestellt hat (z. B. WinPoET), müssen Sie diese Software nach der Installation des Routers nicht mehr ausführen. Möglicherweise müssen Sie Internet Explorer aufrufen und **Tools** (Extras) > **Internet Options** (Internetoptionen) auswählen, auf die Registerkarte **Connections** (Verbindungen) klicken und die Option **Never dial a connection** (Keine Verbindung wählen) aktivieren.

Fehlerbehebung bei PPPoE

Wenn Sie PPPoE verwenden, können Sie Probleme mit Ihrer Internetverbindung über die PPPoE-Verbindung beheben.

➢ **So beheben Sie Fehler bei einer PPPoE-Verbindung:**

1. Melden Sie sich am Router an.
2. Wählen Sie **Management** (Verwaltung) > **Router Status** (Routerstatus).
3. Klicken Sie auf **Connection Status** (Verbindungsstatus). Wenn alle Felder sinnvolle Werte aufweisen, funktioniert die PPPoE-Verbindung fehlerfrei.

Wird bei einem der Schritte ein Fehler oder ein leeres Feld angezeigt, können Sie durch Klicken auf **Verbinden** erneut versuchen, eine Verbindung herzustellen. Der Router versucht immer wieder, eine Verbindung herzustellen.

Wenn Sie nach einigen Minuten immer noch keine Verbindung herstellen können, ist ggf. der verwendete Dienstname, der Benutzername oder das angegebene Kennwort falsch. Möglicherweise liegt auch bei Ihrem ISP ein Problem vor.

Hinweis: Wenn Sie die Verbindung nicht manuell herstellen, findet eine Authentifizierung seitens des Routers über PPPoE erst dann statt, wenn Daten an das Netzwerk übertragen werden.

Fehlerbehebung im Zusammenhang mit dem Internetzugriff

Wenn der Router über eine IP-Adresse verfügt, Sie aber dennoch keine Internet-Websites aufrufen können, kann dies folgende Ursachen haben:

- Ihr Computer erkennt möglicherweise keine DNS-Serveradressen. Ein DNS-Server ist ein Host im Internet, der Internetnamen (z. B. www-Adressen) in numerische IP-Adressen umwandelt.

  Normalerweise stellt der ISP Ihnen die Adressen von einem oder zwei DNS-Servern automatisch zur Verfügung. Wenn Sie bei der Konfiguration des Routers eine DNS-Adresse eingegeben haben, starten Sie den Computer neu.

  Sie können eine DNS-Adresse aber auch nachträglich auf dem Computer festlegen. Hinweise dazu finden Sie in der Dokumentation zu Ihrem Computer.
- Der Router ist auf dem Computer nicht als Standardgateway konfiguriert.

  Starten Sie den Computer neu und stellen Sie sicher, dass die Router-Adresse (www.mywifirouter.com) auf Ihrem Computer als Standardgateway-Adresse eingerichtet wurde.
- Möglicherweise führen Sie für die Anmeldung eine Software aus, die nicht mehr benötigt wird. Wenn Ihnen der ISP ein Programm für die Anmeldung beim Internet zur Verfügung gestellt hat (z. B. WinPoET), müssen Sie diese Software nach der Installation des Routers nicht mehr ausführen. Möglicherweise müssen Sie Internet Explorer aufrufen und Tools (Extras) > **Internet Options** (Internetoptionen) auswählen, auf die Registerkarte Connections (Verbindungen) klicken und die Option Never dial a connection (Keine Verbindung wählen) aktivieren.

Änderungen werden nicht gespeichert

Wenn der Router die über die Router-Benutzeroberfläche vorgenommenen Änderungen nicht speichert, überprüfen Sie die folgenden Punkte:

- Nach der Eingabe der Konfigurationseinstellungen müssen Sie immer auf die Schaltfläche Apply (Übernehmen) klicken, bevor Sie zu einem anderen Bildschirm oder einer anderen Registerkarte wechseln. Anderenfalls gehen Ihre Änderungen verloren.
- Klicken Sie im Webbrowser auf die Schaltfläche **Refresh** (Aktualisieren) bzw. **Reload** (Erneut laden). Es kann sein, dass die Änderungen zwar vorgenommen wurden, im Cache des Webbrowsers jedoch noch die alte Konfiguration gespeichert ist.

Verbindung über WLAN

Wenn Sie Schwierigkeiten haben, eine WLAN-Verbindung mit dem Router herzustellen, versuchen Sie, das Problem zu isolieren.

- Findet das verwendete Wireless-Gerät oder der Computer das WLAN-Netzwerk?

  Falls dies nicht der Fall ist, überprüfen Sie die WLAN-LED an der Vorderseite des Routers. Sie muss leuchten.

  Wenn Sie das SSID-Broadcast des Routers deaktiviert haben, ist das WLAN-Netzwerk versteckt und wird nicht in der Scanliste des WLAN-Clients angezeigt. (SSID ist standardmäßig aktiviert.)
- Unterstützt das Wireless-Gerät die für das WLAN verwendete Sicherheitsoption (WPA oder WPA2)?
- Verwenden Sie ein Netzwerkkabel für den Anschluss eines Computers an einen LAN-Port am Router, um die WLAN-Einstellungen des Routers anzuzeigen. Melden Sie sich dann am Router an, und wählen Sie **Setup** (Konfiguration) > **WiFi Settings** (WLAN-Konfiguration), siehe *WiFi-Setup* auf Seite 24.

  Hinweis: *Klicken Sie anschließend auf **Apply** (Übernehmen), wenn Sie Änderungen vorgenommen haben.*

WLAN-Signalstärke

Wenn das Wireless-Gerät das Netzwerk findet, die Signalstärke jedoch schwach ist, überprüfen Sie die folgenden Punkte:

- Befindet sich der Router zu weit weg oder zu nah am Computer? Stellen Sie den Computer in die Nähe des Routers, jedoch mindestens 1,83 m von ihm entfernt auf, und überprüfen Sie, ob sich die Signalstärke verbessert.
- Wird das WLAN-Signal durch Objekte zwischen dem Router und dem Computer abgeschwächt?

Wiederherstellen der Werkseinstellungen und des Passworts

In diesem Abschnitt wird erklärt, wie Sie die Werkseinstellungen wiederherstellen und damit das Router-Administratorpasswort auf **admin** zurücksetzen. Es gibt zwei Möglichkeiten zum Löschen der aktuellen Konfiguration und Wiederherstellen der Werkseinstellungen:

- Verwenden Sie die Löschfunktion des Routers (siehe *Sichern der Einstellungen* auf Seite 59).
- Betätigen Sie die Reset-Taste an der Rückseite des Routers. Siehe *Werkseitige Voreinstellungen* auf Seite 93. Wenn Sie die Werkseinstellungen wiederherstellen und der Router nicht gestartet werden kann oder die grüne Power-/Test-LED kontinuierlich blinkt, ist das Gerät möglicherweise defekt. Wenn der Fehler sich nicht beheben lässt, liegt möglicherweise ein Hardwarefehler vor. Wenden Sie sich an den technischen Support.

Fehlerbehebung im Netzwerk mithilfe des Ping-Dienstprogramms

Die meisten Netzwerkgeräte und Router verfügen über ein Ping-Dienstprogramm, das ein Echo-Request-Paket an das angegebene Gerät sendet. Das Gerät antwortet dann mit einem Echo-Reply. Die Fehlersuche in Netzwerken wird durch die Verwendung des Ping-Dienstprogramms auf dem Computer oder der Workstation erleichtert.

Testen des LAN-Pfads zum Router

Sie können vom Computer aus ein Ping-Signal an den Router senden, um zu überprüfen, ob der LAN-Pfad zum Router richtig eingerichtet ist.

➢ **So senden Sie von einem Computer unter Windows ein Ping-Signal an den Router:**

1. Klicken Sie in der Windows Symbolleiste auf **Start** und anschließend auf **Run** (Ausführen).
2. Geben Sie im Eingabefeld **ping** gefolgt von der IP-Adresse des Routers ein. Beispiel:

   ping www.mywifirouter.com
3. Klicken Sie auf **OK**.

   Daraufhin sollte eine Nachricht wie die folgende angezeigt werden:

   ```
   Pinging <IP address > with 32 bytes of data (Ping wird ausgeführt
   für <IP-Adresse> mit 32 Byte Daten)
   ```

   Wenn der Pfad funktioniert, wird diese Nachricht angezeigt:

   ```
   Antwort von < IP address >: Bytes=32 Zeit=NNms TTL=xxx
   ```

Wenn der Pfad nicht funktioniert, wird diese Nachricht angezeigt:

```
Zeitüberschreitung der Anforderung
```

Wenn der Pfad nicht richtig funktioniert, könnte eines der folgenden Probleme vorliegen:

- Fehlerhafte physikalische Verbindung

  Achten Sie bei einer Kabelverbindung darauf, dass die nummerierte LAN-Port-LED für den Port, über den die Verbindung besteht, leuchtet.

  Überprüfen Sie, ob die entsprechenden LEDs für Ihre Netzwerkgeräte leuchten. Wenn Router und Computer mit einem separaten Netzwerk-Switch verbunden sind, achten Sie darauf, dass die Verbindungs-LEDs für die mit dem Computer und Router verbundenen Switch-Ports leuchten.

- Fehlerhafte Netzwerkkonfiguration

  Überprüfen Sie, ob die Treiber für die Netzwerkkarte und die TCP/IP-Software auf dem Computer installiert und richtig konfiguriert sind.

  Vergewissern Sie sich, dass die IP-Adressen des Routers und des Computers richtig sind und dass die Adressen zum selben Subnetz gehören.

Testen des Pfads vom Computer zu einem Remote-Gerät

Nachdem Sie sich vergewissert haben, dass die LAN-Pfade einwandfrei funktionieren, sollten Sie den Pfad vom Computer zu einem entfernten Gerät testen.

➢ **So senden Sie ein Ping-Signal:**

1. Klicken Sie in der Windows Symbolleiste auf die Schaltfläche **Start**, und wählen Sie **Run** (Ausführen).
2. Geben Sie im Windows Menü **Run** (Ausführen) die folgende Anweisung ein:

   ping -n 10 <*IP-Adresse***>**

   Setzen Sie dabei anstelle von <IP-Adresse> die IP-Adresse eines entfernten Geräts (z. B. des DNS-Servers des Internet-Providers) ein.

Wenn der Pfad einwandfrei funktioniert, werden dieselben Antworten wie im vorigen Abschnitt angezeigt.

Falls Sie keine Antworten erhalten, überprüfen Sie Folgendes:

- Ihr PC muss eine IP-Adresse aus demselben Subnetz wie der Router haben, der als Standardgateway eingerichtet ist. Wenn die IP-Konfiguration des Computers über DHCP erfolgt ist, werden diese Informationen nicht unter der Option **Network** (Netzwerk) in der Systemsteuerung angezeigt. Vergewissern Sie sich, dass die IP-Adresse des Routers als Standardgateway eingerichtet ist.
- Die Netzwerkadresse des Computers (der Abschnitt der IP-Adresse, der durch die Subnetzmaske festgelegt wird) muss sich von der Netzwerkadresse des entfernten Geräts unterscheiden.

- Das Kabel- oder DSL-Modem muss angeschlossen und in Betrieb sein.
- Wenn der ISP dem Computer einen Hostnamen zugewiesen hat, geben Sie auf dem Bildschirm **Internet Setup** (Internetkonfiguration) diesen Hostnamen als Kontonamen ein.
- Vielleicht akzeptiert der Internet-Provider nur die MAC-Adresse eines einzigen Ihrer Computer und lehnt alle anderen ab.

Viele Breitbandanbieter schränken den Zugang ein, indem sie nur Datenverkehr von der MAC-Adresse Ihres Breitbandmodems zulassen. Manche Internet-Provider schränken den Zugang jedoch noch zusätzlich auf die MAC-Adresse eines einzelnen, an dieses Modem angeschlossenen Computers ein. Wenn dies der Fall ist, konfigurieren Sie Ihren Router so, dass er die MAC-Adresse des berechtigten Computers dupliziert bzw. „fälscht“.

Zusatzinformationen

A

In diesem Anhang werden die folgenden Themen behandelt:

- *Werkseitige Voreinstellungen*
- *Technische Daten*

Werkseitige Voreinstellungen

Tabelle 1. Werkseitige Voreinstellungen des N150R-Routers

Funktion	Voreinstellung
Router-Anmeldung – URL	http://www.mywifirouter.com
Die Router-Anmeldung (Groß- und Kleinschreibung beachten) ist auf dem Typenschild zu finden.	Benutzername: admin Passwort: admin
WAN-MAC-Adresse	Standard-Hardware-Adresse (siehe Typenschild)
MTU-Größe	1500
Die LAN-IP-Adresse ist auf dem Typenschild zu finden (auch als Gateway-IP-Adresse bezeichnet).	192.168.1.1
Router-Subnetz	255.255.255.0
DHCP-Server	Aktiviert
DHCP-Bereich	192.168.1.2 bis 192.168.1.254
Zeitzone	GMT+1: Amsterdam, Berlin, Rom, Wien
Berücksichtigung der Sommerzeit	Deaktiviert
Registrierungsstelle für die Konfiguration des Routers zulassen	Aktiviert
Drahtlose Kommunikation	Aktiviert
SSID-Name (auf dem Typenschild)	OnNetworks*XX*
Sicherheit	*XXXXXXXX*
WLAN-Zugriffsliste (MAC-Filterung)	Alle WLAN-Geräte zugelassen
Netzwerknamen (SSID) übertragen	Aktiviert
Übertragungsgeschwindigkeit	Auto*
Land/Region	USA (nur Nordamerika; ansonsten je nach Land und Region unterschiedlich)
RF-Kanal	Auto
Operationsmodus	Bis zu 150 MBit/s
Übertragungsrate	Bestmöglich
Ausgangsleistung	Vollduplex

Tabelle 1. Werkseitige Voreinstellungen des N150R-Routers (Fortsetzung)

Funktion	Voreinstellung
Eingehend (Daten, die aus dem Internet eingehen)	Gesperrt (alle unerbetenen Anfragen mit Ausnahme des Verkehrs über den HTTP-Port 80 werden abgewiesen)
Ausgehend (Daten, die ins Internet gesendet werden)	Aktiviert (alle ausgehenden Daten können passieren)

**. Maximale Übertragungsrate für Wireless-Geräte gemäß IEEE-Standard 802.11. Der tatsächliche Datendurchsatz hängt von verschiedenen Faktoren ab. Netzwerkprobleme und Umgebungsfaktoren wie Datenvolumen, Baustoffe und Gebäudestruktur sowie Netzwerk-Overhead können den Datendurchsatz beeinträchtigen.*

Technische Daten

Tabelle 2. Technische Daten für den N150R-Router

Funktion	Beschreibung
Daten- und Routingprotokolle	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, BigPond, Dynamisches DNS und UPnP
Netzstecker an Land angepasst	110V-220V, 50/60 Hz, Eingangsspannung
Abmessungen	141,5 x 94 x 30 mm (5,6 x 3,7 x 1,2 in.)
Gewicht	0,137 kg (0,302 lb)
Betriebstemperatur	0 40 °C
Luftfeuchtigkeit	90 % maximale relative Luftfeuchtigkeit, nicht kondensierend
Entsprechend den folgenden Standards hergestellt	FCC Teil 15, Klasse B EN 55022/24 (CISPR 22/24) Klasse B EN 60950 (CE LVD) Klasse B EN 301 489-17 V.2.1.1 (2009) EN 301 489-1 V1.9.2 (2011) EN 300 328 V.1.7.1 (2006) EN 62311: 2008 R&TTE-Richtlinie 99/5/EC ErP 2009/125/EC

Konformitätserklärung

B

WLAN-Router, Gateways, APs

Informationen zur Einhaltung rechtlicher Vorschriften

Hinweis: Dieser Abschnitt enthält die an den Benutzer gestellten Anforderungen für den Betrieb dieses Produkts gemäß der nationalen Gesetze für die Nutzung von Frequenzen und den Betrieb von Funkanlagen. Sollte der Endbenutzer die einschlägigen rechtlichen Vorgaben nicht einhalten, kann dies zu einem rechtswidrigen Betrieb führen, der wiederum dazu führen kann, dass die entsprechende nationale Behörde ein Verfahren gegen den Endbenutzer einleitet.

Hinweis: Die Firmware dieses Produkts beschränkt den Betrieb des Geräts auf die Kanäle, die in den jeweiligen Ländern oder Regionen zulässig sind. Aus diesem Grund stehen möglicherweise nicht alle in diesem Benutzerhandbuch beschriebenen Optionen für Ihre Version des Produkts zur Verfügung.

Europa – EU-Konformitätserklärung

CE

Die Kennzeichnung mit dem o. a. Symbol gibt an, dass die verbindlichen Anforderungen der R&TTE-Richtlinie der Europäischen Union (1999/5/EC) erfüllt werden. Dieses Gerät erfüllt die folgenden Normen:

EN300 328 (2,4 Ghz), EN301 489-17 EN60950-1

Die vollständige Konformitätserklärung finden Sie auf der On Networks-Website mit der EU-Konformitätserklärung unter: *http://www.on-networks.com/do*

EU-Konformitätserklärung in den Sprachen der Europäischen Gemeinschaft

Language (Sprache)	Erklärung
Cesky [Tschechisch]	*On Networks* tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Dänisch]	Undertegnede *On Networks* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch	Hiermit erklärt *On Networks*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estnisch]	Käesolevaga kinnitab *On Networks* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English [Englisch]	Hereby, *On Networks* declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanisch]	Por medio de la presente *On Networks* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Griechisch]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *On Networks* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [Französisch]	Par la présente *On Networks* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italienisch]	Con la presente *On Networks* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Lettisch]	Ar šo *On Networks* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Litauisch]	Šiuo *On Networks* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Niederländisch]	Hierbij verklaart *On Networks* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltesisch]	Hawnhekk, *On Networks* jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Ungarisch]	Alulírott, *On Networks* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polnisch]	Niniejszym On Networks oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portugiesisch]	*On Networks* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slowenisch]	On Networks izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slowakisch]	*On Networks* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnisch]	*On Networks* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [Schwedisch]	Härmed intygar *On Networks* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Isländisch]	Hér með lýsir *On Networks* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegisch]	*On Networks* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Das Gerät ist ein 2,4-GHz-Breitband-Übertragungsgerät (Transceiver), das in allen Mitgliedsstaaten der EU und der EFTA eingesetzt werden darf, mit Ausnahme von Frankreich und Italien, wo nur eine eingeschränkte Nutzung möglich ist.

In Italien sollte der Endbenutzer eine Lizenz bei der nationalen Behörde für Funkfrequenzen beantragen, um eine Genehmigung für die Einrichtung von Funkverbindungen in Außenbereichen und/oder die Bereitstellung von öffentlichem Zugang zu Telekommunikations- oder Netzwerkdiensten zu erhalten.

Dieses Gerät darf in Frankreich nicht für die Einrichtung von Funkverbindungen in Außenbereichen eingesetzt werden, und in manchen Gebieten kann die zulässige äquivalente isotrope Sendeleistung (EIRP) der Funkfrequenzen im Bereich zwischen 2454 und 2483,5 MHz auf 10 mW begrenzt sein. Detaillierte Informationen hierzu sollte der Endbenutzer bei der nationalen Behörde für Funkfrequenzen in Frankreich einholen.

Richtlinien der FCC für den Betrieb in den USA

FCC-Informationen für den Benutzer

Dieses Produkt enthält keine Komponenten, die vom Benutzer gewartet werden können, und darf nur mit dafür zugelassenen Antennen eingesetzt werden. Jegliche Änderungen oder Modifikationen am Produkt führen zum Erlöschen sämtlicher gesetzlicher Zertifizierungen und Zulassungen.

FCC-Richtlinien zur Strahlungsexposition

Die Strahlung dieses Geräts liegt unter den von der FCC festgelegten Grenzwerten für Hochfrequenzstrahlung in einer unkontrollierten Umgebung. Bei der Installation und Verwendung dieses Geräts sollte ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper eingehalten werden.

Dieser Sender darf nicht in der Nähe von oder in Verbindung mit anderen Antennen oder Sendern betrieben werden.

FCC-Konformitätserklärung

Wir, On Networks, 350 East Plumeria Drive, Santa Jose, CA 95134, erklären unter alleiniger Verantwortung, dass der N150 WLAN-Router (N150R) mit Teil 15, Unterabschnitt B der FCC-Vorschriften CFR47 konform ist. Der Betrieb unterliegt den folgenden Bedingungen:

- Dieses Gerät darf keine gesundheitsschädlichen Störungen verursachen und
- Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Operationen verursachen können.

FCC-Warnungen und -Hinweise zu Hochfrequenzstörungen

Dieses Gerät wurde geprüft, und es wurde festgestellt, dass es die Grenzwerte für Digitalgeräte der Klasse B gemäß Teil 15 der FCC-Vorschriften einhält. Diese Grenzwerte sind für die Gewährleistung eines angemessenen Schutzes gegen schädliche Störungen bei der Installation im Wohnbereich gedacht. Dieses Gerät verwendet Funkwellen und kann diese abstrahlen. Wenn es nicht gemäß den Anleitungen installiert und verwendet wird, kann es zu erheblichen Störungen von Funkübertragungen kommen. Bei keiner Installation können Störungen jedoch völlig ausgeschlossen werden. Wenn dieses Gerät Störungen des Rundfunk- und Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Gerätes festgestellt werden kann, sollte der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Platzieren Sie die Empfangsantenne an einer anderen Stelle bzw. richten Sie sie neu aus.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.

- Schließen Sie das Gerät an einen Stromkreis an, den der Empfänger nicht benutzt.
- Wenden Sie sich an den Händler oder einen erfahrenen Rundfunk-/TV-Techniker.

FCC-Warnung

- Veränderungen oder Modifikationen, die nicht ausdrücklich durch die für die Konformität zuständige Stelle genehmigt sind, könnten die Berechtigung des Benutzers zum Betreiben des Gerätes ungültig machen.
- Dieses Gerät ist mit Teil 15 der FCC-Vorschriften konform. Der Betrieb unterliegt den folgenden Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen. (2) Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.
- Produkte für den Markt in den USA können nur auf den Kanälen 1 - 11 betrieben werden. Die Auswahl anderer Kanäle ist nicht möglich.
- Dieses Gerät und die zugehörige(n) Antenne(n) dürfen nicht in der Nähe von oder in Verbindung mit anderen Antennen oder Sendern betrieben werden.

Kanadisches Ministerium für Kommunikation (Department of Communications) – Vorschriften zu Funkstörungen

Dieses digitale Gerät (N150 WLAN-Router (N150R)) überschreitet nicht die Grenzwerte der Klasse B für von digitalen Geräten ausgehende Funkstörungen, wie sie in den Vorschriften zu Funkstörungen des kanadischen Ministeriums für Kommunikation festgelegt sind.

Dieses Digitalgerät der Klasse [B] entspricht dem kanadischen Standard ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

Dieses Gerät stimmt mit RSS-210 der Regeln von Industry Canada überein. Der Betrieb unterliegt den folgenden Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen. (2) Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.

WICHTIGER HINWEIS: Erklärung zur Strahlenbelastung:

Die Strahlung dieses Geräts liegt unter den von IC festgelegten Grenzwerten für Hochfrequenzstrahlung in einer unkontrollierten Umgebung. Bei der Installation und Verwendung dieses Geräts sollte ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper eingehalten werden.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Tabelle für die Reduzierung von Funkstörungen

In der nachfolgenden Tabelle wird der empfohlene Mindestabstand zwischen On Networks-Geräten und -Haushaltsgeräten zur Reduzierung von Funkstörungen angegeben (in Metern und Fuß).

Haushaltsgerät	Empfohlener Mindestabstand (in Metern und Fuß)
Mikrowellengeräte	9 Meter (30 Fuß)
Babyfon – analog	6 Meter (20 Fuß)
Babyfon – digital	12 Meter (40 Fuß)
Schnurloses Telefon – analog	6 Meter (20 Fuß)
Schnurloses Telefon – digital	9 Meter (30 Fuß)
Bluetooth-Geräte	6 Meter (20 Fuß)
ZigBee	6 Meter (20 Fuß)

Stichwortverzeichnis

A

Access Points 71
Adressen, DNS 22
Adressreservierung 33
Advertising-Periode 80
Aktualisieren der Firmware 57
Änderungen nicht gespeichert, Router 88
Angeschlossene Geräte, anzeigen 65
Anmelden
    ISP 12
Anmeldung
    Arten 14
    Firmware aktualisieren 13
    Passwort ändern 60
    Router 13
Anwendungen, QoS für Online-Spiele 35
Automatisch an Sommer-/Winterzeit anpassen 43
automatische Internetverbindung 16

B

Basisstation, konfigurieren 73
Benutzerdefinierter Dienst (Portweiterleitung) 52

C

Contentfilter 39
Crossover-Kabel 84
CTS/RTS-Grenzwert 68

D

Datenpakete, fragmentiert 28
Deaktivieren
    SSID-Broadcast 23
DHCP-Server 32
Dienste 42
DMZ-Server 28
DMZ-Standardserver 28
DNS-Adressen
    Fehlerbehebung 86
DNS-Server 47
DNS-Serveradressen (Domain Name Service) 22
Domain Name Server (DNS), sekundär 22
Domain Name Server (DNS)-Adressen 22
DSL-Porteinstellungen 62
Dynamisches DNS 75
DynDNS.org 75

E

eingehenden Datenverkehr, zulassen oder sperren 46
E-Mail-Benachrichtigungen 45

F

Fehlerbehebung 81
    Routeränderungen nicht gespeichert 88
Fernsteuerung 78
Filtern von Inhalten 39
Firewall-Ausgangsregeln 40
Firewall-Eingangsregeln 40
Firewalls
    Eingangsregeln 40
Firmware, aktualisieren 57
    bei Anmeldung 13
    manuell 58
fragmentierte Datenpakete 28
Fragmentierungslänge 68
Funk, drahtlos 68
Funkkanal 26

G

Gateway-IP-Adresse 21
Grundeinstellungen (Bildschirm)
    Beschreibung 21

H

Hinzufügen
    Benutzerdefinierter Dienst 52
    Prioritätsregeln 35
Host, vertrauenswürdig 42
Hostname 21

I

Internet Relay Chat (IRC) 48
Internet Service Provider (ISP), siehe ISP
Internetanschluss, keine Verbindung 17
Internet-LED, Fehlerbehebung und 83
Internet-Port 16
Internetseiten, sperren 41
Internetverbindung
  Fehlerbehebung 85
IP-Adresse
  DHCP 12
IP-Adressen
  dynamisch 75
  reserviert 33
ISP
  Grundeinstellungen (Bildschirm) 21
  Kontodaten 12
ISP-Anmeldung 12

K

Kabel, prüfen 82
Keine Internetverbindung 17
Konfiguration sichern 60
Konfiguration, WLAN 24
Konfigurationsdatei löschen 60
Konfigurationsdatei, verwalten 60
Konfigurieren
  DMZ-Server 28
  Dynamisches DNS 76
  NAT 28
  Port-Triggering 53
  QoS 34
  Repeater 74
konfigurieren
  Portweiterleitung 51
Konformität 95

L

LAN-Konfiguration 30
LAN-Port
  QoS für 36
LAN-Ports 63
Lebensdauer, Advertising 80
LEDs
  Beschreibung 9
  Fehlerbehebung und 83
Liste der zugriffsberechtigten WLAN-Karten 69
lokale Server, Portweiterleitung zu 51

M

MAC-Adressen
  Beschreibung 23
  QoS für 37
  Typenschild 10
Manuelle Abmeldung 14
Menüs, Beschreibung 15
Metrikwert 78
Modemeinstellungen, Status 63
MTU-Größe 28
Multicasting 31

N

NAT (Network Address Translation) 28, 47
Network Time Protocol (NTP) 43
Netzwerk neu starten 82
Netzwerk, Vorgehensweise bei Neustart 82
Netzwerke
  Zugriffssteuerung 40
Netzwerke, Fehlerbehebung 82
Netzwerkkabel, prüfen 82
Netzwerk-LED, Fehlerbehebung und 83, 84

O

Online-Hilfe, Router 15

P

Pakete, fragmentiert 28
Passphrasen 26
  Typenschild 10
Passwort, wiederherstellen 89
Passwortwiederherstellung, admin 61
Point-to-Point Tunneling Protocol (PPTP) 16
Portnummern 42
Ports
  Filtern 40
  Weiterleitung 40
Ports,aufgelistet, Rückseite 9
Port-Triggering 46, 48, 50, 53
Portweiterleitung 46, 49, 50, 51
Positionieren des Routers 7
Power-LED, Fehlerbehebung und 83
PPPoE (PPP over Ethernet) 86
Präambelmodus 68
Primäre DNS-Adressen 22
Priorität des Datenverkehrs 34

Protokolle 66
Protokolle, per E-Mail senden 45

Q

QoS (Quality of Service) 34

R

Repeater 74
Reservierte IP-Adressen 33
Router, Status 62
Router-Benutzeroberfläche, Beschreibung 15
Rückseite 9

S

Sekundärer DNS 22
Senden von Protokollen per E-Mail 45
Seriennummer, Typenschild 10
Setup-Assistent 16
Sicherheit 23
Sicherheitsfunktionen 23
Sicherheitsoptionen 24
Sicherheitsoptionen, Beschreibung 24
Sicherheits-PIN 10, 18
Simple Mail Transfer Protocol (SMTP) 45
Sperren
    eingehenden Datenverkehr 46
Sperren mit Stichwörtern, Beispiele 41
Sperren von Inhalten und Diensten 39, 41
Spiele, Online, QoS für 35
SSID
    Beschreibung 26
    Deaktivieren 23
Statische Routen 76
Statistik, anzeigen 64
Status
    Internetverbindung 65
    Router 62
Stichwörter, Datenverkehr sperren durch 41
Syslog 66

T

TCP/IP
    Keine Internetverbindung 17
Typenschild, Produkt 10

U

Über WLAN verbinden 7
Universal Plug and Play (UPnP) 79

V

Verpackungsinhalt 7
Vertrauenswürdiger Host 42
Verwalten des Routers über Remote-Zugriff 78
Virtual Channel Identifier (VCI) 12
Virtual Path Identifier (VPI) 12
Vorderseite 8
Voreingestellte Sicherheit 22
Voreingestellte Sicherheitsfunktionen 26
Vorhandenen Router austauschen 12

W

WAN-IP-Adresse, Fehlerbehebung 85
WAN-Konfiguration 27
Warnmeldungen, per E-Mail senden 45
Werkseinstellungen
    zurücksetzen 10
Werkseinstellungen, wiederherstellen 89
Werkseitige Voreinstellungen, wiederherstellen 89
Wiederherstellen
    Konfigurationsdatei 60
    Werkseitige Voreinstellungen 89
Wiederherstellen des Administratorpassworts 61
Wi-Fi Protected Setup (WPS) 17
    Geräte, hinzufügen 17
Wireless Distribution System (WDS) 71, 72
Wireless LAN (WLAN) 64
Wireless-Geräte,hinzufügen zum Netzwerk 17
Wireless-Sicherheit 23
Wireless-Verbindung, Fehlerbehebung 88
WLAN 68
WLAN-Einstellungen 26
WLAN-Konfiguration 24
    SSID-Broadcast 25
    Überprüfen auf Richtigkeit 82
WLAN-Konfiguration (Bildschirm) 24
WLAN-LED, Fehlerbehebung und 85
WLAN-Netzwerkname (SSID)
    Typenschild 10
WLAN-Port-Konfiguration 63
WLAN-Radius 7

WLAN-Region 26
WLAN-Repeater 71, 72
  Basisstation 73
  Repeater 74
WLAN-Sicherheitsoptionen 24
WLAN-Übertragungsmodus 26
WLAN-Verbindungen 7
WMM (Wi-Fi Multimedia) 34

Z

zeitliche Bestimmung 43
Zeitüberschreitung, Port-Triggering 55
Zeitzone festlegen 43
Zeitzone, festlegen 43
Zugreifen auf Remote-Computer 46
Zugriff
  Remote 78
Zugriffssteuerung
  Aktivieren 70